



Who's Behind This Website?

Updated March 2024



<https://bit.ly/nicar24-behind-this-website>

Priyanjana Bengani
Senior Research Fellow
Tow Center for Digital Journalism
@acookiecrumbles@indieweb.social

Jon Keegan
Investigative Data Journalist
The Markup
@jonkeegan@mastodon.social

Agenda

- Asking the right questions: Who? Why?
When? How?
- Where to begin?
 - Site content
 - Infrastructure & Networking
 - Connections with Platforms
- Case studies - (Content warning)
- Tools & resources

The new normal: more opacity, less transparency

Existing tools are breaking

- Google Cache no longer exists
- Google dorks / search operators are less reliable
- Dnslytics' tools have moved to “legacy”

Concealing identities is easier

- WHOIS is less useful for new domains due to GDPR
- Squarespace, Wordpress, GoDaddy static websites share IP addresses with thousands of websites
- CDNs make IP address matching harder
- Relatively easy to incorporate a company incognito or with false identities

World of platforms and walled gardens

- Google Analytics 4 disallows finding relationships between websites based on the ID
- Platforms are restricting their transparency tools (TikTok, Twitter, the imminent death of CrowdTangle)
- Far more platforms (Mastodon, BlueSky, Threads, Discord, ...) to monitor
- Facebook’s “Related Pages” no longer work

**Somebody set this
website up!
Who? Why? When? How?**



Who?

Who's featured on the website?

Are there authors? Email addresses? Profile pictures?

Are there payment options (crypto, PayPal, donations, subscriptions)? Who's receiving the money?

Are authors common across multiple sites or exclusive to this one?

Is the owner trying to stay hidden?

Why?

Why was this website set up?

To make money through scams or ads (content farms)?

To perform some kind of influence operations?

To promote political candidates or social advocacy?

To deceive the audience by impersonating another website?

When?

When was the domain first registered?

How long has the site existed in its current form?

Was it offline for any significant period of time?

Did the ownership change? (Check historical WHOIS)

Did the site's design or content change drastically at any point?

How?

What is the tech stack?

Where is it hosted?

Wordpress? (Check authors, templates, plugins)

How is the site monetized? Affiliate links, advertising?

Is the content generated by AI?

Where does it link to, and who links to it?

Documenting, archiving, monitoring

YOU NEED TO BE ABLE TO **RETRACE YOUR STEPS** AND HAVE ALL THE **RECEIPTS**
ESPECIALLY IN AN ENVIRONMENT WHERE **EVERYTHING CHANGES ALL THE TIME**

Documenting

- Maintain a **data diary** with detailed notes about what you've looked at and how you got there
- Try to **create a timeline** of the website and how it's evolving over the course of your investigation
- Use **Hunchly** or screen recordings to keep track of everything you're doing

Monitoring

- Set up **Klaxon Cloud** or **VisualPing** to be notified of any changes to a site
- Use GitHub Actions and **ShotScraper** for automated screenshots over time

Archiving

- Archive sites consistently, and in some cases, use multiple archival services (archive.org, archive.is)
- For **public records** or **social media posts**, take screenshots — some of them might not be archivable
- **Download videos** lest they get taken down (Youtube: [yt-dlp](#))
- Take **screenshots with timestamps** so you can monitor changes and gather receipts ([GoFullPage](#)).
- Capturing the **full browser window with the URL** field helps strengthen your evidence

So many tools

A word about investigative tools...

TECHNIQUES > TOOLS

- Spend time learning solid, creative investigative techniques
- Most of the time, you'll have to use multiple tools — even if they purport to do the same thing!
- There are SO many tools, and they come and go
- Tools can be expensive, overpromise, underdeliver — and use dubious means to collect data
- Platforms rise and fall, APIs go away
- Don't get too dependent on one tool

The screenshot shows the homepage of whotwi, a service for graphical Twitter analysis. At the top right is a yellow button labeled "Start my free 30-day trial". Below it is the whotwi logo with the tagline "Graphical Twitter Analysis". A message states "whotwi has ended service on April 4, 2023. Why? Thank you very much for your long term visit since 2011." The main content area is a grid of cards:

- For any questions/suggestions pls reach out to:** [@lorandbodo.com](https://twitter.com/lorandbodo)
- FOSINT**: A curated list of useful online FOSINT resources.
- Case Studies**: Financial investigations
- Company Information**: A curated list of Company Information Databases
 - Escavador
 - The KYC Registry
 - Databases (Worldwide) – OpenGazettes.com
 - OpenCorporates :: The Aleph data search
 - Overseas registries
- Country Profile**: Guides to history, politics and economic background of militaries, countries and territories.
 - BBC NEWS
 - Country – Libya
 - Refworld | Libya
 - Country Anti Money Lau...
 - The World Factbook
 - Country Profiles | Annex...
 - World Media Directory ...
 - Get World News by RSS ...
 - Foreign travel advice
 - European Country of Ori...
 - Country Profiles
 - Libya Immigration Deten...
 - Passport Index
 - pi PublicIntelligence.net
 - International - U.S. Ener...
- Aviation Movements**: A curated list of tools to identify aircrafts and track/monitor aviation
 - VIS
 - Kuuru
- Training & Tutorials**: OSINT Handbook 2018
 - LibGuides: Intelligence S...
 - OSINT: How to find Infor...
 - Magma.lavallof.org
 - Learn - Google Earth Ou...
 - Investigations KIT
 - BIRD - BIRN Investigati...
 - Bird.tools
 - Security Education Com...
 - Detecting Fake Viral Sto...
 - Citizen Investigation Gui...
 - Intro to I2P
 - We Are OSINTcurious
 - OSINT Handbook 2018
 - Exposing the Invisible
 - Casefile - Visualization ...
 - Verification Handbook: h...
 - comp3321 NSA Python ...
 - Research Clinic
 - CNS New Tools Coursew...
 - Dark Web Tools
 - GUIN - Toolbox
 - European Country of Ori...
 - Coronavirus: Resources ...
 - VIS
 - Kuuru
- Live Social**: CrowdTangle
- Blogging, forum & other c...**: A curated list of blogs, forums and other communities by Bellingcat/Techniclette.
 - Strava
 - Tumblr
 - LiveJournal
 - Classmates
 - Wordpress
 - Blogger
 - Wix
 - Medium
 - ProBoards
 - SquareSpace
 - Joomla
 - Ghost
 - Weebly
- Radio**: A curated list of Radio resources by Bellingcat/Techniclette.
 - Listen to Live ATC (Air Tr...
 - Radarreference
 - Broadcastify
 - Radio.garden
 - SDR.hu
 - GlobalTuners
 - ProScan
 - MIScaners
 - Tuneln
 - Live Online Radio
 - Radio Garden
- TV**: Vidgrid.tk.gq
- Hacking resources**: Adversary.crowdstrike.c...
- Dating Apps & Sites**: A curated list of dating apps
 - Adversary.crowdstrike.c...

<https://start.me/p/7kxyy2/osint-tools-curated-by-lorand-bodo>

Protecting yourself online

Each investigation will have a different **threat model**

If you don't want to **expose your IP address** to the website:

- Use a VPN or Tor (note: some VPNs also track your activity!)
- Use a browser different to your primary browser in incognito / private mode

If you don't want to **expose your email address** to the website:

- Use a different email address when you sign up to newsletters
- Ensure your email client blocks remote content from loading to avoid pixel tracking
- Use the '+' trick to see if your email address is shared with other services

If you need to use a virtual machine, use [UTM](#) or [VMWare](#)

Is it ethical? Is it legal?

SPEAK TO YOUR **EDITORS** and **LAWYERS**!

MAKE SURE YOUR INVESTIGATION IS IN **THE PUBLIC INTEREST**.

Ethics

- Some tools collect data using shady practices — say buying data from data brokers — and purchasing these tools may help sustain these businesses (...which we probably should be reporting on...)
- At times, identifying who's behind a website might end up in doxing someone's identity — which is complicated

⚠️ Be aware of crossing lines while trying to access data: while publicly-available sites are largely fine, using unauthorized credentials is a legal concern

😢 But, also, note: the St Louis Post-Dispatch reporter who found SSNs exposed by simply “viewing source” on Missouri’s Department of Elementary and Secondary Education’s (DESE) website was accused of “hacking”

Legal

- If you’re scraping publicly-available content, you’re *probably* fine but should still be aware of the Computer Fraud and Abuse Act.

Site content

Content: Text

Check **text fragments** from articles, “about us” pages, and privacy policies to see if they are unique to the site or duplicated [[Use exact string matching on multiple search engines](#)]

Run article text through numerous tools to see if the text is **AI-generated**, but note lots of false positives in these tools [[GPTZero](#), [OpenAI's Text Classifier](#), [ContentScale's AI Detector](#), [CopyLeaks](#)]

Browse site for any names (including bylines), email addresses, phone numbers, addresses, social media handles, and company names

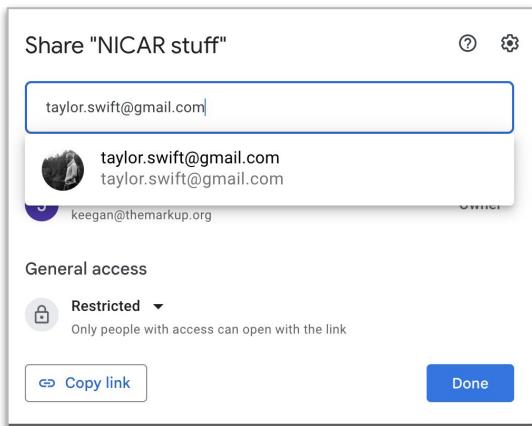
On finding names, or phone numbers, or e-mail addresses, or...

- ➡️ Use tools like [Epieos](#) and [haveibeenpwned](#) to **reverse lookup emails and phone numbers**: both will show you other services and platforms on which the email address or phone number might exist. [TrueCaller](#) also serves as a **reverse phone book**.
- 🔍 If you find **social media handles**, use tools like [sherlock](#) that will scan multiple platforms to see if the same handle appears elsewhere — you'll still have to confirm that it's the same user and not just the same handle
- 👤 If you find names, use Bellingcat's [Name Variant Tool](#) to find possible variations on any names
- 🏢 If you find **company names**, use [OpenCorporates](#) or [LinkedIn](#) to see whether any personnel information is available. OpenCorporates also lets you **search by addresses** — so you can find who else shares the same office location!

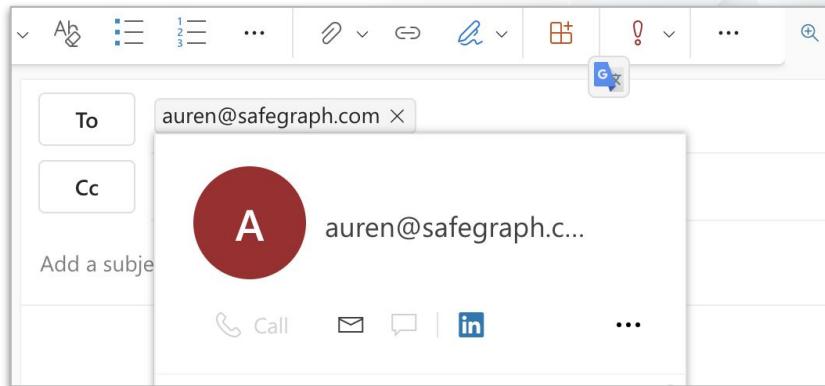
Given an email address...

If you find a Gmail address and the other tools don't give you a break, enter the address in Google Docs' sharing sheet. If the address is valid, you should see a profile picture.

⚠ Remember to not actually share the document!



If you want to find a LinkedIn profile associated with an email address, compose an email in Outlook, and put the address in the “To” field.



Content: Media

 Use [reverse image search](#) across multiple platforms (Google, Bing, Yandex) to check:

- If image is a stock image
- If the profile picture for an author appears elsewhere
- If the image is posted on other sites

 Use [facial recognition tools](#) ([PimEyes](#), [Search4Faces](#), [FaceCheck.ID](#), [Amazon Rekognition](#)) to see if it can identify faces in the profile pictures

 Use [EXIF tools](#) ([EXIF Data](#)) to check:

- If any metadata is retained in the images. This can include location, time the photograph was taken, camera details, etc

 Use [forensics tools](#) to check:

- If media is AI-generated [[WeVerify \(InVid\)](#)]
- If media has been modified from the original [[Forensically](#)]

Content: Documents

Google dorking

To find documents that might be hosted on your website, use Google dorking:
`filetype:pdf site:<domain_of_interest.com>`. Also try XLS, XLSX, PPT, DOC

If you find a PDF, open it (ideally in a browser) and check document details / information for any names. And check PDF metadata. Use [Dangerzone](#) or [Google Drive](#) if you are worried about malware.

Amazon S3

Look at the website's source to see if there's anything hosted on AWS S3. The bucket name can be revealing, and the [bucket might be open](#) if misconfigured.

Donations, Memberships, Subscriptions

PayPal

💳 If there's a PayPal button, click through until you finally get to the screen that tells you who you're about to pay. If the PayPal account has been banned, you can still try the PayPal link in Internet Archive.

Crypto

💸 Lookup the wallet address in search engines to see where else they show up

Lookup the wallet address in [crypto investigation tools](#) ([EtherScan](#), [Breadcrumbs](#)) to see how much money it has and how active it is

Others

💰 Websites might have a plethora of payment services — from gaming platforms to AliPay — and sometimes it's worth going through all the steps to see what information you can find out about the payee. ([Case study](#): Behind a Secretive Global Network of Non-Consensual Deepfake Pornography)

WordPress Websites

Use [wpscan](#) to see the **theme** a Wordpress site uses as well as the **authors**

WordPress Themes and plugins are often used across networks of sites. Check [Built.with](#)

```
| Found By: Rss Generator (Passive Detection)
|   - https://empirenews.net/feed/, <generator>https://wordpress.org/?v=6.4.3</generator>
|   - https://empirenews.net/comments/feed/, <generator>https://wordpress.org/?v=6.4.3</generator>

[+] WordPress theme in use: empire-news
| Location: https://empirenews.net/wp-content/themes/empire-news/
| Readme: https://empirenews.net/wp-content/themes/empire-news/README.md
| Style URL: https://empirenews.net/wp-content/themes/empire-news/style.css?ver=6.4.3
| Style Name: empire news
| Description: Empire News theme...
| Author: Jitender Thakur

| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)

| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
|   - https://empirenews.net/wp-content/themes/empire-news/style.css?ver=6.4.3, Match: 'Version: 1.0'
```

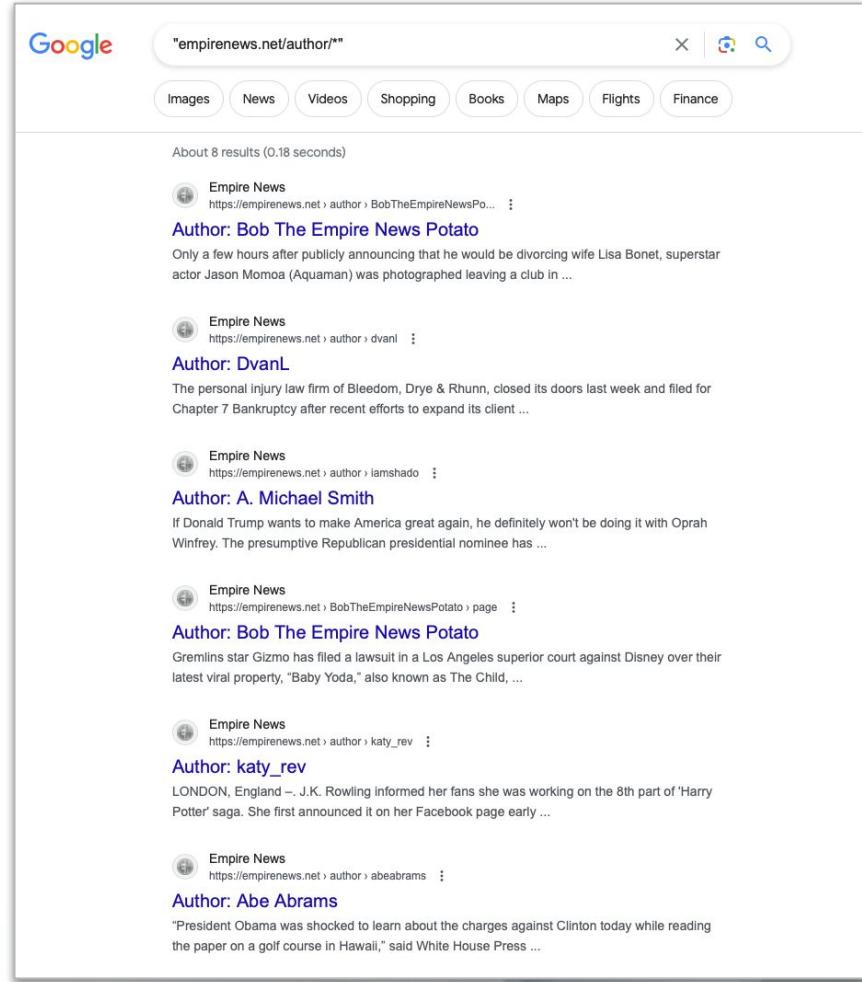
<https://wpscan.com/>

WordPress Websites

Use the Google author trick:
["empirenews.net/author/*"](https://empirenews.net/author/*)

Pulling RSS feeds can sometimes show you authors

You can pull RSS article links into Google Sheets
using [IMPORTFEED](#)



A screenshot of a Google search results page. The search query is "empirenews.net/author/*". The results list several news articles from Empire News, each attributed to a specific author:

- Author: Bob The Empire News Potato**
Only a few hours after publicly announcing that he would be divorcing wife Lisa Bonet, superstar actor Jason Momoa (Aquaman) was photographed leaving a club in ...
- Author: DyanL**
The personal injury law firm of Bleedom, Drye & Rhunn, closed its doors last week and filed for Chapter 7 Bankruptcy after recent efforts to expand its client ...
- Author: A. Michael Smith**
If Donald Trump wants to make America great again, he definitely won't be doing it with Oprah Winfrey. The presumptive Republican presidential nominee has ...
- Author: Bob The Empire News Potato**
Gremilins star Gizmo has filed a lawsuit in a Los Angeles superior court against Disney over their latest viral property, "Baby Yoda," also known as The Child, ...
- Author: katy_rev**
LONDON, England ~. J.K. Rowling informed her fans she was working on the 8th part of 'Harry Potter' saga. She first announced it on her Facebook page early ...
- Author: Abe Abrams**
"President Obama was shocked to learn about the charges against Clinton today while reading the paper on a golf course in Hawaii," said White House Press ...

Internet Archive

To get the lay of the land of a website, look at the URLs tab of the website, which shows all the URLs Internet Archive has captured, along with dates and number of captures.

This [waybackurls.py](#) script will do this for you quickly.

INTERNET ARCHIVE										
DONATE			Explore more than 866 billion web pages saved over time reuterstoday.com							
Calendar • Collections • Changes • Summary • Site Map • URLs										
934 URLs have been captured for this URL prefix.										
Filter results by URL or MIME Type (e.g.: .txt)										
URL 1										
http://reuterstoday.com/										
http://reuterstoday.com/favicon.ico										
http://reuterstoday.com/robots.txt										
https://reuterstoday.com/robots.txt?infodev&subdir=1&list=2										
https://reuterstoday.com/stop-a_18157B_893c_8.html										
https://reuterstoday.com/guomod_cdc.html										
https://reuterstoday.com/OPX/Signature/fe437767.html										
https://reuterstoday.com/Preference-mat_click_idh302197391.html										
https://reuterstoday.com/Preference-umat_click_idh302197391.html										
https://www.reuterstoday.com/										
https://www.reuterstoday.com/8-billion-awarded-to-india-in-2023.html										
https://www.reuterstoday.com/10-top-black-friday-items-to-watch-out-for-in-2023.html										
https://www.reuterstoday.com/20-years-after-us-met-south-korea-in-1953-what-is-the-future.html										
https://www.reuterstoday.com/20-years-after-us-met-south-korea-in-1953-what-is-the-future.html										
https://www.reuterstoday.com/2021-cricket-world-cup.html										
https://www.reuterstoday.com/2023-7-round-trip-must-reads.html										
https://www.reuterstoday.com/2023-bnp-paribas-open.html										
https://www.reuterstoday.com/2023-circus-tour-speakers.html										
https://www.reuterstoday.com/2023-coronavirus-pandemic.html										
https://www.reuterstoday.com/2023-euro-pepsi.html										
https://www.reuterstoday.com/2023-financial-markets.html										
https://www.reuterstoday.com/2023-financial-markets.html										
https://www.reuterstoday.com/2023-govt-budget.html										
https://www.reuterstoday.com/2023-holiday-travel.html										
https://www.reuterstoday.com/2023-india-urination-case-sharake-maths-fells-dehi-court-woman-peed-on-her-own-seat.html										
https://www.reuterstoday.com/2023-india-urination-case-sharake-maths-fells-dehi-court-woman-peed-on-her-own-seat.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										
https://www.reuterstoday.com/2023-india-vietnam-trade-agreement.html										

<https://web.archive.org/web>

Reuters Today and BBC News Today were identified by [Bleeping Computer](#) as part of a content farm impersonating major news outlets

Infrastructure and networking

When it comes to domains, we need to ask

👤 Ownership

Who owns the domain?

What other domains do they own?

What network is it a part of, if any?

💥 Shared traits

Which other domains share the IP addresses?

Which domains share tracking & adtech identifiers?

Which domains share SSL certs or favicons?

🌐 Links and network requests

Which domains do they link to?

Which domains link to it?

Where do images and other media load from?

💰 Adtech

Which countries' ad-tech platforms are used?

Who are the top advertisers / advertising platforms?

Who owns the domain? What other domains do they own?

Lookup the [WHOIS data](#) for the domain (current and historic)

GDPR has made this useless for new domains, but Whoxy provides historic domain registration details

Even if registration details are obscured, you still see [when a domain was registered](#) and with [whom](#)

People can lie in WHOIS — it's up to the domain registrar to check

To find other possible related domains, use [dnstwist](#), which gives you domain permutations

Tools: [Whoxy](#), [RiskIQ](#), [DomainTools](#), [DNSTwist](#)

The screenshot displays four separate WHOIS records for the domain `mexicobusinessdaily.com`, each with a different timestamp in a dark green box:

- 20 NOV 2019**:
 - Name: Registration Private ([136 million domains](#))
 - Company: Domains By Proxy, LLC ([187 million domains](#))
 - Email: mexicobusinessdaily.com@domainbyproxy.com
 - Country: United States ([226 million domains](#)) from United States for **\$6,000**
 - Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
 - Status: clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
- 1 JUN 2022**:
 - Name: Privacy Administrator ([1.88 million domains](#)) [\[UPDATED\]](#)
 - Company: Anonymize, Inc. ([2.34 million domains](#)) [\[UPDATED\]](#)
 - Email: mexicobusinessdaily.com-urgs42cabtx@anonymize.com [\[UPDATED\]](#)
 - Country: United States ([226 million domains](#)) from United States for **\$6,000**
 - Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
 - Status: clientTransferProhibited [\[UPDATED\]](#)
- 10 AUG 2022**:
 - Name: Privacy Administrator ([1.88 million domains](#))
 - Company: Anonymize, Inc. ([2.34 million domains](#))
 - Email: mexicobusinessdaily.com-u6ogn28nid2@anonymize.com [\[UPDATED\]](#)
 - Country: United States ([226 million domains](#)) from United States for **\$6,000**
 - Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
 - Status: clientTransferProhibited
- 10 APR 2023**:
 - Name: Privacy Administrator ([1.88 million domains](#))
 - Company: Anonymize, Inc. ([2.34 million domains](#))
 - Email: mexicobusinessdaily.com-trdfvq4y7vq@anonymize.com [\[UPDATED\]](#)

<https://www.whoxy.com/>

Which other domains share the IP addresses?

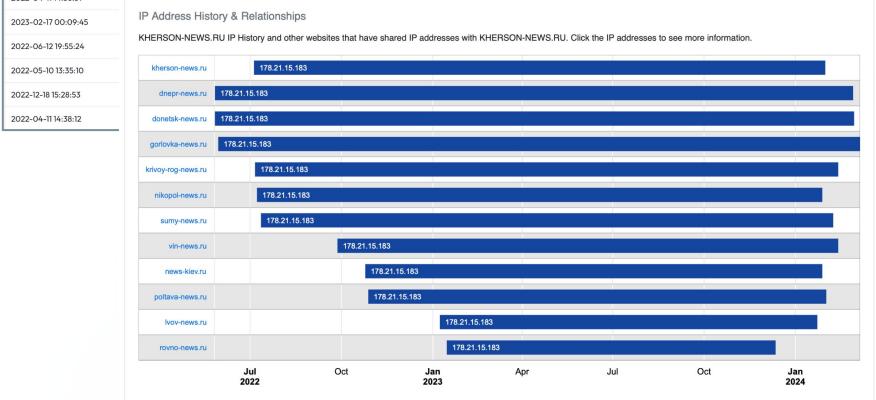
Find the current and historic IP addresses of the domain.

Find what other domains reside — or have resided — on the same IP address over what time period

If the IP address is Cloudflare or Google Cloud or GoDaddy, matching IP addresses aren't a reliable indicator — if you get thousands of results, abort!

Tools: [Built.With](#), [SecurityTrails](#), [RiskIQ](#), [DomainTools](#), [FarSight DNSDB](#)

TIME FIRST SEEN	TIME LAST SEEN	COUNT	RRNAME	RRTYPE	RDATA
2022-04-19 19:46:43	2024-03-07 09:32:32	202205	donetsk-news.ru.	A	178.21.15.183
2022-04-19 19:20:21	2024-03-07 09:04:49	11502	nikopol-news.ru.	A	178.21.15.183
2022-04-19 19:11:20	2024-03-07 08:58:13	612193	kherson-news.ru.	A	178.21.15.183
2022-04-05 15:45:33	2024-03-07 08:52:12	114641	dnepr-news.ru.	A	178.21.15.183
2022-04-06 19:21:24	2024-03-07 08:32:49	364312	news-kiev.ru.	A	178.21.15.183
2022-12-18 15:28:44	2024-03-07 05:12:56	31011	lvov-news.ru.	A	178.21.15.183
2022-04-04 19:50:58	2024-03-07 03:21:50	20825	sumy-news.ru.	A	178.21.15.183
2022-12-18 15:32:28	2024-03-07 05:09:49	10328	rovno-news.ru.	A	178.21.15.183
2022-04-19 20:30:18	2024-03-07 00:29:44	10421	krivoy-rog-news.ru.	A	178.21.15.183
2022-06-09 14:56:17	2024-03-07 00:26:36	15791	poltava-news.ru.	A	178.21.15.183
2022-04-11 14:37:29	2024-03-06 22:48:14	488	www.kherson-news.ru.	A	178.21.15.183
2022-04-25 18:19:55	2024-03-06 22:28:55	64129	gorlovka-news.ru.	A	178.21.15.183
2022-04-04 20:01:11	2024-03-06 21:11:49	10720	vin-news.ru.	A	178.21.15.183
2022-04-11 14:36:31					
2023-02-17 00:09:45					
2022-06-12 19:55:24					
2022-05-10 15:35:10					
2022-12-18 15:28:53					
2022-04-11 14:38:12					



<https://built.with> & DNSDB Scout

Which other domains share the same analytics identifiers?

Identify third-party analytics and tracking libraries used by the website. These include Google Analytics, Facebook Pixel, Quantcast, NewRelic, Google Tag Manager, etc.

Find other domains that share the same identifiers

Tools: [RiskIQ](#), [BuiltWith](#)

Hostname	First Seen	Last Seen
lonestarstandard.com	2020-11-22	2024-03-04
centroplexnews.com	2021-06-08	2024-03-04
amarillogazette.com	2020-10-11	2024-03-04
centraltxnews.com	2020-10-11	2024-03-04
bentontimes.com	2020-10-19	2024-03-02
abilenetmes.com	2020-07-04	2024-01-28
fayettevillesandard.com	2023-07-08	2023-07-19
jonesborotimes.com	2023-06-06	2023-06-06
nwarkansasnews.com	2022-05-31	2022-05-31
naturalstatenews.com	2021-06-28	2021-07-27

<https://community.riskiq.com>

A note about Google Analytics

Google Analytics IDs used to be in the syntax **UA-NUMBER-SUFFIX**. Related domains shared the same **UA-NUMBER**, but the SUFFIX was different.

Google Analytics 4 changes this such that each website has different identifiers

Bellingcat's [Wayback Analytics](#) tool looks at Internet Archive to extract old analytics IDs, which might be helpful in the present and can be used to aid the investigation

```
"someurl.com": {
    "current_UA_code": "UA-12345678-1",
    "current_GA_code": "G-1234567890",
    "current_GTM_code": "GTM-12345678",
    "archived_UA_codes": {
        "UA-12345678-1": {
            "first_seen": "01/01/2019(12:30)",
            "last_seen": "03/10/2020(00:00)"
        },
        ...
    },
    "archived_GA_codes": {
        "G-1234567890": {
            "first_seen": "01/01/2019(12:30)",
            "last_seen": "01/01/2019(12:30)"
        }
    },
    "archived_GTM_codes": {
        "GTM-12345678": {
            "first_seen": "01/01/2019(12:30)",
            "last_seen": "01/01/2019(12:30)"
        }
    }
},
```

Links

Find who's linking to the website of interest consistently by using a [backlink checker \(ahrefs, Moz\)](#) — what's the relationship between the sites?

Use [photon](#) or [urlscan.io](#) to gather the [outbound urls](#), (urls a site links to), as well as some high-level "intel" — who's the site linking to the most?

Analyze outbound links, especially those to merch stores, for [affiliate links](#) — who's the affiliate? (Especially useful for health and wellness scams)

Backlink profile for eprimefeed.com

Domain including subdomains. One link per domain

Domain Rating: 37

Backlinks: 34K
78% dofollow

Linking websites: 12K
91% dofollow

DR	Referring page	Anchor and target URL
96	Electronic stability control - Wikipedia	"Itelma is ready to supply ABS and ESC units to all car factories in Russia". https://en.wikipedia.org/wiki/Electronic_stability_control
93	Pertes humaines de la guerre russo-ukrainienne — Wikipédia	« American mercenary Andrew Cooper destroyed in Artemovsk on the "Road of Life" KXan 36 Daily News - ePrimefeed », https://fr.wikipedia.org/wiki/Pertes_humaines_de_la_guerre_russo-ukrainienne
0	Activate all versions of Office 2016 for FREE permanently	Archives https://eprimefeed.com/archives/
7	CARA BERMAIN UKULELE SENAR 3 ~ Yoki Mirantiyo	Archives https://eprimefeed.com/archives/
	Till Lindemann: Frauen, Skandale, aktuelle	heute offen. Es wäre sein viertes Kind. Im April 2022 behauptete allerdings ein Konzertproduzent, dass sowohl die Beziehung als auch die

<https://ahrefs.com/backlink-checker>

Tracking, Analytics, AdTech

Analyzing the stack

Which ad trackers, third-party cookies, and other creepy surveillance libraries is the site using?

This might provide some insight into the motivations behind the site.

Tools: [Blacklight](#), [BuiltWith](#)

Blacklight Inspection Result

Blacklight works by visiting each website with a headless browser running custom software built by The Markup. To learn more, read our [methodology](#).

5 Ad trackers found on this site.
This is **less than** the average of **seven** that we found on popular sites

5 Third-party cookies found.
This is **more than** the average of **three** that we found on popular sites

 Tracking that evades cookie blockers wasn't found.

 This website could be monitoring your keystrokes and mouse clicks.
Blacklight detected the use of a session recorder, which tracks user mouse movement, clicks, taps, scrolls, or even network activity. This data is compiled into videos and heat maps that website owners can watch to see how users interact with the site. Research has shown these practices can be insecure and make sensitive user data such as passwords and credit card information more vulnerable to leaks. This technique was used by fifteen percent of popular websites when we [scanned them](#) in September 2020.

Blacklight detected a script belonging to the company **Yandex LLC** doing this on this site.
However...
While Blacklight can detect whether a session recorder was loaded, it cannot determine exactly how the collected data is being used.
[How We Define This](#)

 We did not find this website capturing keystrokes.

<https://themarkup.org/blacklight>

Tracking, Analytics, AdTech

Monitoring network requests

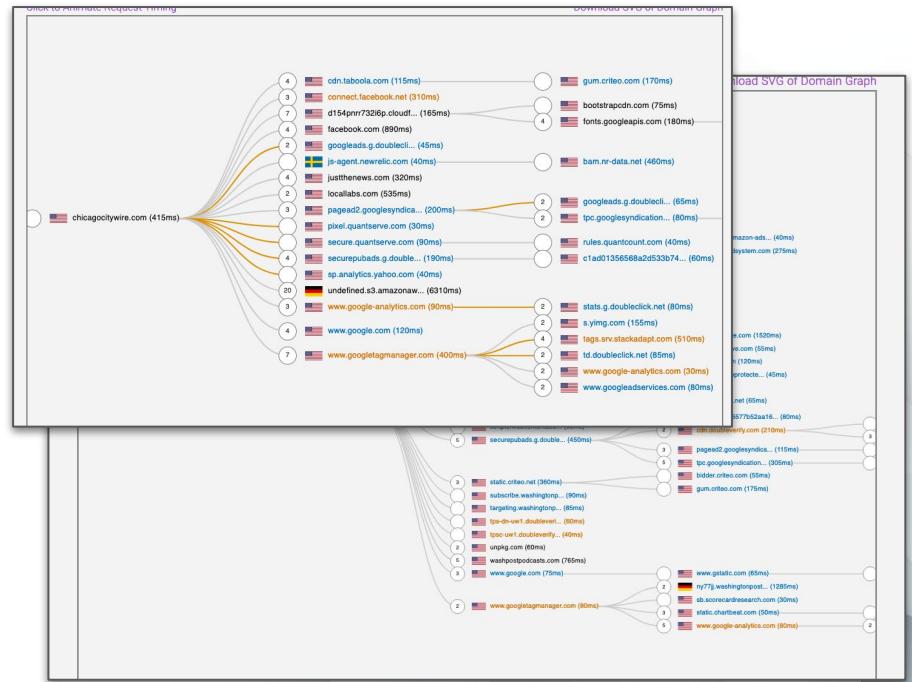
Is the site making network calls to ad-tech providers in other countries?

Is the url for its static files (images, videos) different to the website?

Are there any network calls that warrant further investigation? (Check the Network tab in developer tools)

Who are the top advertisers?

Use [FouAnalytics X-Ray](#) to see all the network requests a site makes.



<https://pagexray.fouanalytics.com/>

Connections to platforms

When it comes to platforms, we need to ask

TOO MANY PLATFORMS, TOO LITTLE TIME



Individual platform

- On which platforms does the domain get high traction? And is it on the domain's account or elsewhere?
- Which other accounts does it interact with?
- What other domains does it promote?
- Does it look like engagement was purchased?
- Where else does the profile picture appear?
- Does the account appear to have been co-opted at any point?



Presence on other platforms

- Even if not listed on the site, is there presence on other platforms?
- Tools like [Sherlock](#) and [Blackbird](#) help you find other social media accounts



Ads

- Are there ads featuring the domain on any platforms?
- Which entity has run those ads?

Facebook Page Transparency

On any Facebook Page, go to “About” and then “Page Transparency,” and then click on “See All”

- largely pointless as it could be a notable entity or it could be someone who paid Meta
- addresses can be plugged into OpenCorporates to see which other entities share the address
- useful to understand where page managers are located, and if that aligns with what the page says it does

These fields are typically only filled in for companies or pages running ads

<https://facebook.com/>

The screenshot shows the "Page transparency" interface for "The New York Times". At the top, it says "Page information for The New York Times". Below that is the page's logo and name, "The New York Times", with a blue checkmark and the description "Media/news company". A section titled "Organizations that manage this Page" shows "New York Times Co is responsible for this Page", described as a person or organization that has completed verification. A "Verified" badge is highlighted in red, explaining that accounts with it are authenticated using trusted documentation. It also mentions a "Meta Verified" subscription for proactive account protection and increased prominence. The page's location is listed as "NEW YORK NY, 10018161B United States of America". A "History" section shows it was created by "The New York Times" on October 29, 2007. A "People who manage this Page" section shows the primary location is the United States, with smaller populations in Costa Rica and the United Kingdom. A "Ads from this Page" section indicates the page is currently running ads and has run ads about social issues, elections, or politics. Buttons for "Go to Ad Library" and "Find support or report Page" are at the bottom, along with a "Close" button.

Case studies

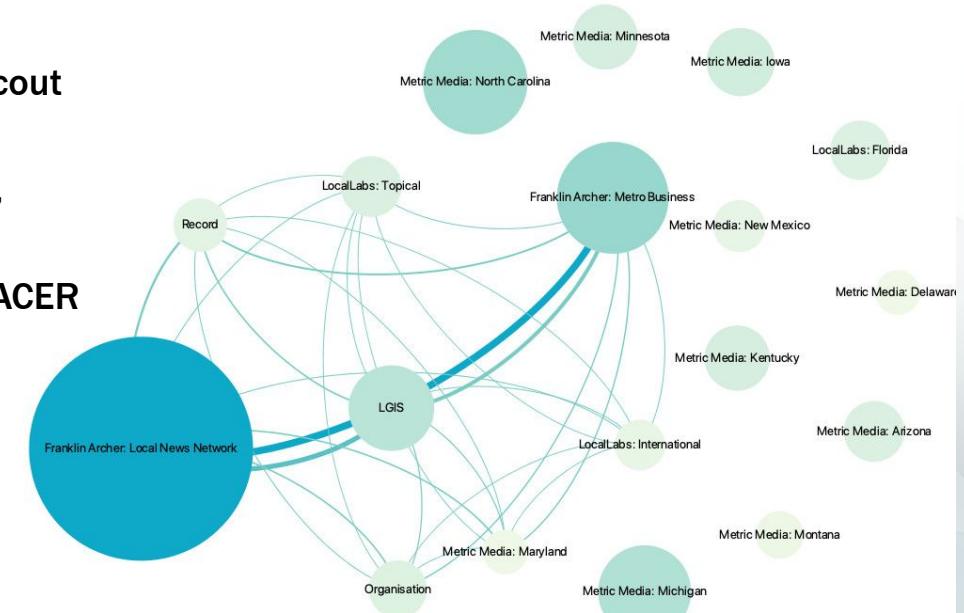


Investigating politically-backed “pinkslime” local news

<https://aitestkitchen.withgoogle.com/tools/image-fx>

- Analyzing domains: **RiskIQ**, **FarSight DNSDB Scout**
- Analyzing matching analytics: **RiskIQ**
- Following the money: **OpenSecrets**, **FEC filings**, **state records**, **990s**
- Corporate ownership web: **OpenCorporates**, **PACER**
- Collaborations & partners:
Facebook and Google Ad Library,
DNSDB Flexible Search

https://www.cjr.org/tow_center_reports/hundreds-of-pink-slime-local-news-outlets-are-distributing-algorithmic-stories-conservative-talking-points.php



Dozens of new websites appear to be Michigan local news outlets, but with political bent

Carol Thompson | Lansing State Journal
Updated 1:53 AM EST Dec 12, 2019

LANSING — Dozens of websites branded as local news outlets launched throughout Michigan this fall, with monikers like Lansing Sun, Ann Arbor Times, Thumb Reporter and UP Gazette, promising local news but also offering political messaging.

The nearly 40 new sites present a challenge for readers navigating a digital media environment that has unlimited space for publishing stories that are hard to distinguish as journalism, advocacy or political messaging.

About us

Welcome to Metric Media LLC. Our origin began in 2014 by filling the growing news void in local and community news after years of steady disinvestment in local reporting by legacy media. We were founded by a group of people deeply committed to addressing the growing news desert at the local level. This site is one of hundreds and eventually thousands that we are launching nationwide to fill that void in local and community news.

Local, state and federal governments operate today without any media oversight in most of the U.S., a trend that is worsening. When citizens are deprived of basic government information and accurate perspective, communities and civic discourse suffer.

Our reporting philosophy is to provide objective, data-driven information without inserting personal or political viewpoints and biases into our stories. We let the facts speak for themselves.

We also strive to give voice to the voiceless and powerless, those whose opinions on critical issues are now rarely heard. That especially includes the "unorganized"—entrepreneurs, small business owners, property taxpayers and parents who don't benefit from lobbyists and public relations consultants.

If you want a voice in your community, we want to hear from you.



How do you find the thousands of political outlets launching to fill the void in local and community news?

Looking up the IP addresses of a couple of domains in **DNSDB Scout** yielded over a thousand results!

Show 25 entries				To Unicode	Invert	Export
Filter Time First	Filter Time Last	Filter Count	Filter RRName	Filter RRTypE	Filter RDatA	
Time First Seen	Time Last Seen	Count	RRName	RRTypE	RDatA	
2020-01-18 18:21:08	2020-09-06 03:06:46	199	youngstowntimes.com.	A	3.218.216.245	
2020-01-18 19:34:12	2020-09-03 18:08:43	203	wcindiananews.com.	A	3.218.216.245	
2020-01-18 18:16:41	2020-09-03 13:13:30	217	whitewatertimes.com.	A	3.218.216.245	
2020-01-18 18:16:48	2020-09-03 07:32:56	172	weststarknews.com.	A	3.218.216.245	
2020-01-18 18:16:43	2020-09-03 07:30:28	228	westlucasnews.com.	A	3.218.216.245	
2020-01-18 19:34:21	2020-09-03 07:30:10	190	westindynews.com.	A	3.218.216.245	
2020-01-18 18:17:47	2020-09-03 07:30:02	215	westhamiltonnews.com.	A	3.218.216.245	
2019-09-15 13:13:30	2020-09-03 07:29:49	582	westernwaynetoday.com.	A	3.218.216.245	
2020-01-21 18:25:20	2020-09-03 07:29:05	211	westclevelandnews.com.	A	3.218.216.245	
2020-01-18 18:16:47	2020-09-03 06:18:56	207	wcwisconsinnews.com.	A	3.218.216.245	
2019-09-08 20:00:29	2020-09-03 06:18:40	686	wcmichigannews.com.	A	3.218.216.245	
2020-01-18 18:24:07	2020-09-03 06:08:23	269	waynecountytoday.com.	A	3.218.216.245	
2020-01-18 18:16:41	2020-09-03 06:06:31	202	waukeshatimes.com.	A	3.218.216.245	
2019-09-08 20:00:36	2020-09-03 06:05:03	562	waterfordtoday.com.	A	3.218.216.245	
2020-01-18 18:16:46	2020-09-03 05:55:09	213	washingtoncotimes.com.	A	3.218.216.245	
2019-09-05 20:25:08	2020-09-03 05:53:47	780	warrensun.com.	A	3.218.216.245	
2020-01-18 18:16:45	2020-09-03 05:53:39	223	warrenclintonnews.com.	A	3.218.216.245	
2019-09-05 21:14:25	2020-09-03 02:33:22	754	thumbreporter.com.	A	3.218.216.245	
2020-01-18 18:16:47	2020-09-03 01:46:18	186	vacationlandtimes.com.	A	3.218.216.245	
2019-09-05 21:14:44	2020-09-03 00:56:20	758	upgazette.com.	A	3.218.216.245	
2020-01-18 18:16:42	2020-09-02 23:00:14	187	tuscarawasnews.com.	A	3.218.216.245	
2020-01-21 05:55:15	2020-09-02 22:17:35	227	trumballnews.com.	A	3.218.216.245	
2020-01-18 18:20:32	2020-09-02 21:45:18	252	triconews.com.	A	3.218.216.245	
2019-09-08 19:32:33	2020-09-02 21:45:05	617	tricitysun.com.	A	3.218.216.245	
2020-01-18 18:32:27	2020-09-02 19:58:40	206	toledoreporter.com.	A	3.218.216.245	

1 to 25 of 137 Results

Show 25 entries				To Unicode	Invert	Export
Filter Time First	Filter Time Last	Filter Count	Filter RRName	Filter RRTypE	Filter RDatA	
Time First Seen	Time Last Seen	Count	RRName	RRTypE	RDatA	
2020-09-05 04:28:11	2022-03-23:33:53	118	southernnewsnetwork.com.	A	34.236.176.60	
2020-08-31 08:51:16	2022-03-23:29:07	591	ftworthtimes.com.	A	34.236.176.60	
2020-08-28 23:26:10	2022-03-23:27:44	539	easthoustonnews.com.	A	34.236.176.60	
2020-08-27 22:00:03	2022-03-23:25:35	5319	centralutahnews.com.	A	34.236.176.60	
2020-09-09 06:08:33	2022-03-23:19:43	5815	nefranklinnews.com.	A	34.236.176.60	
2020-09-13 19:01:03	2022-03-23:08:57	16685	southdaytonnews.com.	A	34.236.176.60	
2020-08-30 01:37:56	2022-03-22:57:45	6275	lowedeltanews.com.	A	34.236.176.60	
2020-08-24 15:07:46	2022-03-22:55:38	3358	jonesborotimes.com.	A	34.236.176.60	
2020-09-14 03:50:39	2022-03-22:55:00	3633	larimernews.com.	A	34.236.176.60	
2020-08-26 03:37:43	2022-03-02:22:54:52	7815	eastclevelandnews.com.	A	34.236.176.60	
2020-08-21 09:38:04	2022-03-02:22:51:33	6183	beehivestate.com.	A	34.236.176.60	
2020-09-03 18:08:43	2022-03-02:22:51:14	4171	southutahnews.com.	A	34.236.176.60	
2020-09-04 09:56:58	2022-03-02:22:49:21	159	northokcnews.com.	A	34.236.176.60	
2020-08-24 19:10:08	2022-03-02:22:45:16	493	coachella.com.	A	34.236.176.60	
2020-09-16 05:44:25	2022-03-02:22:41:54	128	westoctor.com.	A	34.236.176.60	
2020-09-10 06:08:28	2022-03-02:22:40:56	393	tulsastandard.com.	A	34.236.176.60	
2020-09-16 10:44:44	2022-03-02:23:33:19	9300	sekentuckynews.com.	A	34.236.176.60	
2020-09-11 17:26:10	2022-03-02:22:32:33	160	phillyleader.com.	A	34.236.176.60	
2020-08-21 09:06:35	2022-03-02:22:25:30	3171	annarbor.com.	A	34.236.176.60	
2020-09-16 23:22:50	2022-03-02:22:03:08	15366	swgeorgianews.com.	A	34.236.176.60	
2020-09-14 17:14:11	2022-03-02:21:56	7617	nesacramentonews.com.	A	34.236.176.60	
2020-09-15 04:53:10	2022-03-02:21:28	6005	nepiedmontnews.com.	A	34.236.176.60	
2020-09-12 13:09:50	2022-03-02:21:48:44	3870	georgiamountainnews.com.	A	34.236.176.60	
2020-08-24 18:26:12	2022-03-02:18:23	4922	ibxnews.com.	A	34.236.176.60	
2020-09-07 04:06:48	2022-03-02:21:41	1708	southpimanews.com.	A	34.236.176.60	

1 to 25 of 960 Results

Putting each domain through RiskIQ to find tracking identifiers (Google, Facebook, NewRelic), we identified ~1,300 domains

The screenshot shows the RiskIQ platform interface. At the top, there's a search bar with the query "ua-147552306". Below the search bar, the text "ua-147552306 (GoogleAnalyticsAccountNumber)" is displayed. On the left, there's a sidebar with sections for "DATA", "Filters", "HOSTNAME (39 / 39)", "TAG", and "SYSTEM TAG". The "HOSTNAME (39 / 39)" section lists several domains with checkboxes and counts: annarbortimes.c... (1), battlecreektimes... (1), detroitcitywire.c... (1), discuss.httparchi... (1), downrivertoday.... (1). A "Show More" link is present. The main area shows a table with columns for "Hostname" and "First Seen". Some rows are expanded to show more details.

The screenshot shows two RiskIQ interface instances side-by-side. The top instance has a search bar with "ua-58698159" and displays "ua-58698159 (GoogleAnalyticsAccountNumber)". It shows a table with "Tracker Search: Hosts" (61) and "Tracker Search: IP Addresses" (31). The bottom instance has a search bar with "eec005bb88" and displays "eec005bb88 (NewRelicId)". It also shows a table with "Tracker Search: Hosts" (171) and "Tracker Search: IP Addresses" (372). Both instances have sections for "DATA", "Filters", and "HOSTNAME (25 / 25)". The tables list various hostnames along with their first seen dates and last seen dates.

PIPELINE MEDIA LLC

Company Number LLC_02632055

Native Company Number 02632055

Status Goodstanding

Incorporation Date 10 November 2008 (over 15 years ago)

Company Type Limited Liability Company

Jurisdiction Illinois (US)

Registered Address 2045 W. GRAND AVE. STE B

CHICAGO

60612

IL

United States

Previous Names
LOCALITY LABS, LLC
JOURNALIC, LLC
BLOCKSHOPPER LLC

Alternative Names PIPELINE MEDIA SERVICES LLC (trading name, 2021-07-15 -)

Agent Name L. ROBERT PASQUESI

Agent Address 585 BANK LN. STE 3000, LAKE FOREST, Sangamon, 60045

Directors / Officers CAMERON, BRAD, manager

DUNN, TIMOTHY, manager

L. ROBERT PASQUESI, agent

TIMPONE, BRIAN, manager

Registry Page <https://apps.llsos.gov/corporatelc/>
Website unavailable outside U.S.

Events for PIPELINE MEDIA LLC

- On 2008-11-10 Incorporated
- Between 2008-11-10 and 2022-11-07 Addition of officer CAMERON, BRAD, manager
- Between 2008-11-10 and 2022-11-07 Addition of officer DUNN, TIMOTHY, manager
- Between 2008-11-10 and 2022-11-07 Addition of officer L. ROBERT PASQUESI, agent
- Between 2008-11-10 and 2022-11-07 Addition of officer TIMPONE, BRIAN, manager



🤔 How do you confirm this is actually the West Texas oil billionaire who's heavily involved in Texas politics and he already has existing close ties to the network?



⌚ When did Dunn get involved with this network?

ANALYSIS

As election looms, a network of mysterious ‘pink slime’ local news outlets nearly triples in size

AUGUST 4, 2020
By PRIYANJANA BENGANI



CJR PARTNER TOW CENTER

‘Pink slime’ network gets \$1.6M election boost from PACs backed by oil-and-gas, shipping magnates

OCTOBER 31, 2022
By PRIYANJANA BENGANI



TOW REPORT

Hundreds of ‘pink slime’ local news outlets are distributing algorithmic stories and conservative talking points

DECEMBER 14, 2021
By PRIYANJANA BENGANI

Advocacy groups and Metric Media collaborate on local ‘community news’

OCTOBER 14, 2021
By PRIYANJANA BENGANI

TOW REPORT

The Metric Media network runs more than 1,200 local news sites. Here are some of the non-profits funding them.

OCTOBER 14, 2021
By PRIYANJANA BENGANI

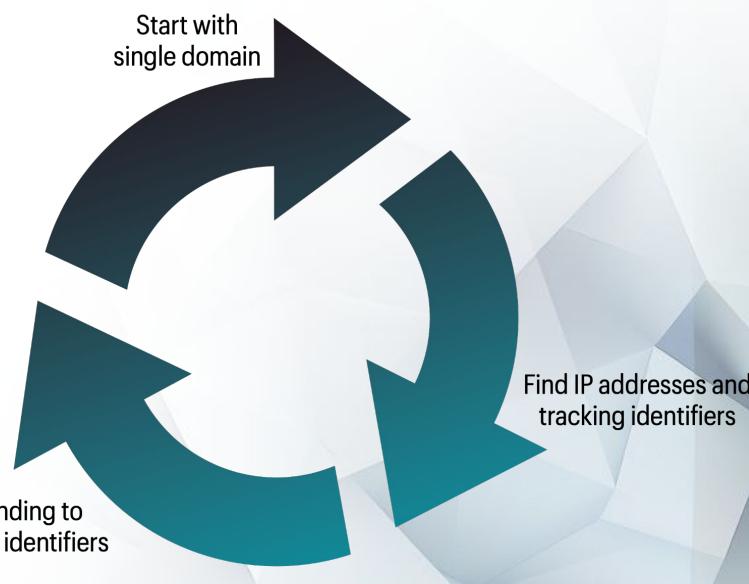


Everything that goes into the story has to be verified — maybe manually

Just because you identified a person's name doesn't necessarily mean you found the "right" person

Google obsessively — you never know when something new comes up

Document everything, things change rapidly, and if you don't have the receipts, you can't rely on your memory!



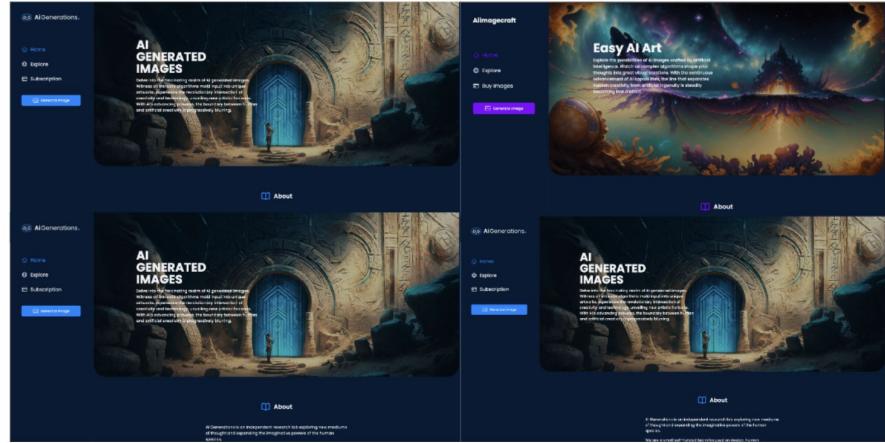
Find domains corresponding to
IP addresses and tracking identifiers

Start with
single domain

Find IP addresses and
tracking identifiers

Bellingcat: Pornographic Deepfake Sites

By Kolina Koltai



<https://www.bellingcat.com>

- Analyzing domains: **DomainTools**
- Analyzing photographs
- Following the money across payment and e-commerce platforms: **Steam, G2A, PayPal, Shopify, Coinbase, Patreon, Venmo, Stripe**
- Revealing hidden information from archives
- Investigating business records in several regions
- Connecting social media profiles: **Facebook, LinkedIn, VKontakte**
- Identifying AI generated images and text
- Following network redirects

[bell^{ling}cat](#) Investigations Guides Ukraine Justice & Accountability Workshops EN [Donate](#)



Kolina Koltai
Kolina Koltai is a senior researcher and trainer at Bellingcat. An expert in how sociotechnical systems influence the decision making of social groups, she received her PhD from the University of Texas's School of Information, has previously worked at the Center for an Informed Public at the University of Washington.

Behind a Secretive Global Network of Non-Consensual Deepfake Pornography

February 23, 2024 Deepfakes Finance

Warning: This article discusses explicit adult content and child sexual abuse material (CSAM)

One of the world's largest online video game marketplaces says it has referred user accounts to legal authorities after a Bellingcat investigation found tokens to create nonconsensual pornographic deepfakes were being surreptitiously sold on the site. Accounts on G2A were being used to collect payments for *Clothoff*, one of the most popular and controversial nonconsensual pornographic deepfake sites on the internet. *Clothoff* disguised the sales as if they were for downloadable gaming content.

"Security is one of our top priorities that we never compromise on, hence we have taken immediate action and suspended the sellers in question until we have investigated it fully," G2A said, in a statement. "We also decided to report the case to the appropriate authorities." (G2A said it was reporting the accounts and the companies affiliated with them to authorities in the "companies' countries of origin" which, as this story outlines below, varies but includes the US and New Zealand.)

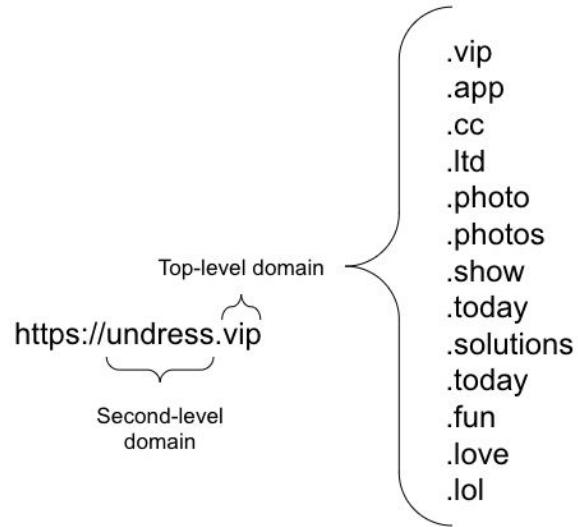
Clothoff is part of a loosely affiliated network of similar platforms uncovered in Bellingcat's investigation.

The network, which also includes the sites *Nudify*, *Undress*, and *DrawNudes*, has variously manipulated financial and online service providers that ban adult content and non-consensual deep fakes by disguising their activities to evade crackdowns. Other services they have tried to exploit include Coinbase, Patreon, Paypal, Shopify, Steam and Stripe.

<https://www.bellingcat.com/news/2024/02/23/behind-a-secretive-global-network-of-non-consensual-deepfake-pornography>

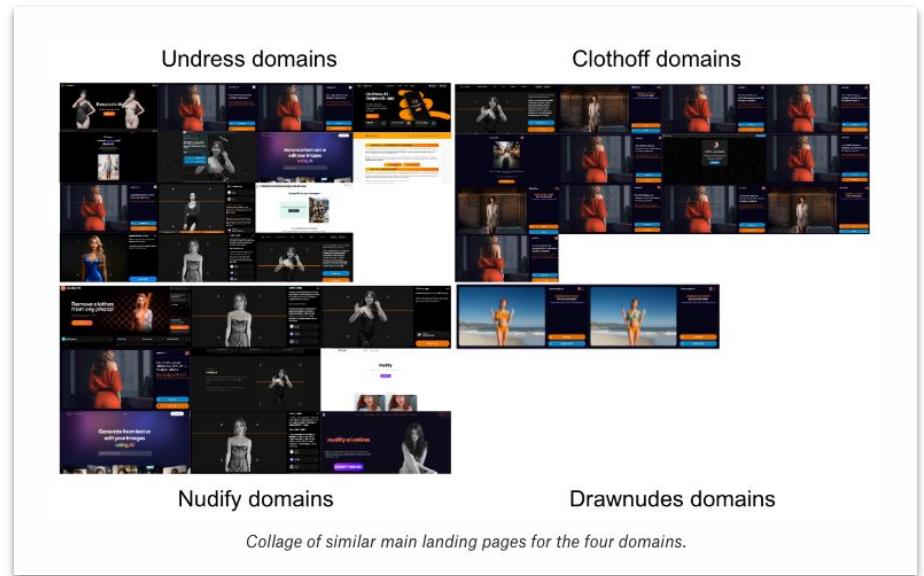
- Accounts on videogame marketplace G2A sold tokens to use on non-consensual pornographic deepfake site
- A network of these sites shared similar TLDs — this is the kind of scenario where [dnstwist](#) could be useful
- Sites redirected to each other

This is illustrated below, where you can see some of the multiple TLDs of Undress.

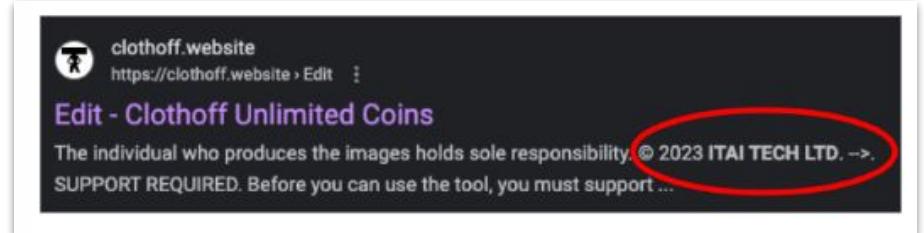


An example of the Top-Level Domains (TLDs) on the Second-Level Domain (SLD) 'Undress' (Bellingcat).

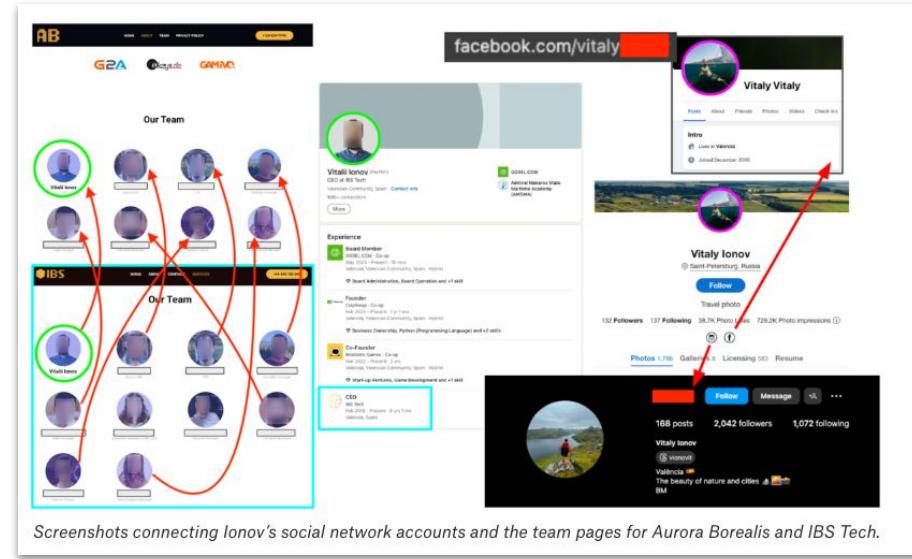
- Looking at all the domains for the sites revealed shared layouts and photographs
- A Google cache* archive of the sites shared a common company listed
- Payment pages for each site all shared the same design and template
- An analysis using RiskIQ revealed a dedicated server IP for multiple deepfake sites



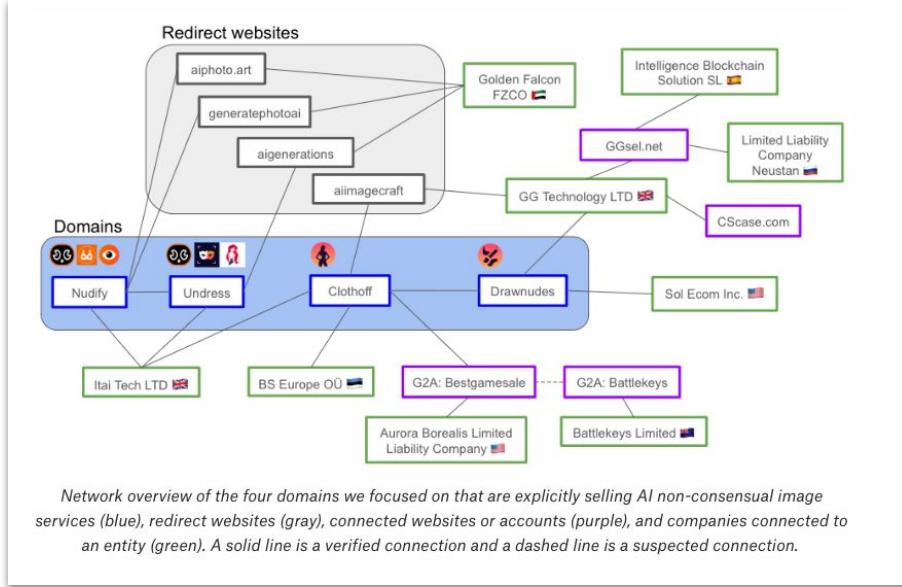
* Google just removed all cached pages from search results 🤦



- Examining business registrations found connections between companies linked to the deepfakes sites
- Using “dealers” as middlemen to broker token transactions on mainstream payment platforms, the companies were able to evade detection
- Telegram bots prompted buyers how to jump through hoops to process payments



- Taken together these connections provide strong evidence of a network of entities seeking to obscure its owners, disguise transactions and evade detection
- *“However, these organisations have not perfectly covered their tracks. There are real people who have lent their names, and even their companies, to these platforms.”*



Resources

Newsletters

Craig Silverman's [Digital Investigations](#)

[Digital Digging](#) with Henk van Ess

Jack Creps' [The OSINT Newsletter](#)

Excellent books

[Verification Handbook](#) edited by Craig Silverman

Michael Bazzell's [Open Source Intelligence Techniques](#)



Thank you!

<https://bit.ly/nicar24-behind-this-website>

<https://github.com/jonkeegan/behind-this-website>



Jon Keegan

Investigative Data Journalist

The Markup

@jonkeegan@mastodon.social

Priyanjana Bengani

Senior Research Fellow

Tow Center for Digital Journalism

@acookiecrumbles@indieweb.social