

Domain and Business Name OSINT:

Advanced Operators and webtools

Search Operator	Function	Example
Site:	Search for results from a particular website.	site:apple.com "steve jobs" site:trellis.com "gomez" AND "los angeles"
site:* .domain.coim	Uses google as a subdomain enumerator	site:*.vrcinvestigations.com
intitle:	Search for pages with a particular word in the title tag.	intitle:housefire
Filetype:	Searches by filetype Searches by filetype at targeted domain	Filetype:pdf vrcinvestigations.com Site: vrcinvestigations.com filetype:pdf

The above boolean operators can be combined and manipulated to target multiple queries like domain and name, domain and location, business name and location, etc. Below are web tools that automate this search process for you. All booleans can be useful for business/domain searches; however, the above are the most useful queries for domains and business names.

Investigator.io

<https://abhijithb200.github.io/investigator/>

Chrome Extension 1:

<https://chromewebstore.google.com/detail/dork-search-tool/neadoiokjghjpklekpjifhheaddbdjca?hl=en>

Chrome Extension 2:

<https://chromewebstore.google.com/detail/dork-it/lnihadedihlhjcbnimcobnppdlldocm?hl=en>

Shodan & Censys:

Shodan and Censys can be used to geolocate websites by locating their server endpoints. This allows us to use location as an identifier for a website/business domain.

Shodan:

Example with location highlighted:

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

47.190.47.224

vrclinvestigation
s.com

Frontier
Communications
of America, Inc.

United
States, Denton

SSL
Certificate

Issued By:
|- Common
Name:
RapidSSL TLS
RSA CA G1
|- Organization:
DigiCert Inc

Issued To:
|- Common
Name:
*.vrclinvestigations.com

Supported SSL
Versions:
TLSv1.2

HTTP/1.1 302 Found

Content-Type: text/html; charset=UTF-8

Location: <https://vrclinvestigations.com>

Server:

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: default-src 'self'; script-src 'self';

X-Content-Security-Policy: default-src 'self'; script-src 'self';

X-Content-Type-Options: n...

2024-12-15T13:15:17.188709

Censys:

Example with location highlighted:

47.190.47.200

As of: Dec 16, 2024 9:13pm UTC | Latest

Summary

History

WHOIS

Explore

Raw Data

Basic Information

Reverse DNS

mail.vrclinvestigations.com

Forward DNS

mail.vrclinvestigations.com

Routing

47.190.0.0/17 via FRONTIER-FRTR, US (AS5650)

OS

microsoft windows

Services (2)

443/HTTP, 500/IKE

Labels

NETWORK.DEVICE.VPN

HTTP 443/TCP

12/14/2024 12:15 UTC

Software

microsoft windows

VIEW ALL DATA

GO

Details

https://47.190.47.200/

Status

200 OK

Body Hash

sha1:1de0bcd974930ada7ac58ffbd7bb48c751c1d73

Response Body

EXPAND

Geographic Location

City

Denton

State

Texas

Country

United States (US)

Coordinates

33.21484, -97.13307

Timezone

America/Chicago

Whois/Domain Registration:

Below are tools that link domains to registration names and phone numbers. The functionality of these tools are limited and often lead to redacted or unusable information. IF a result IS found, you'll be able to find registration emails and phone numbers for a website. Normally the records containing useful information are from early on in a websites history (normally the creation) so historic tools are required for consistently effective searches. I have this ability with OSINT tools. One solid webtool is featured as an example and the others are listed.

View DNS info:

<https://viewdns.info/>

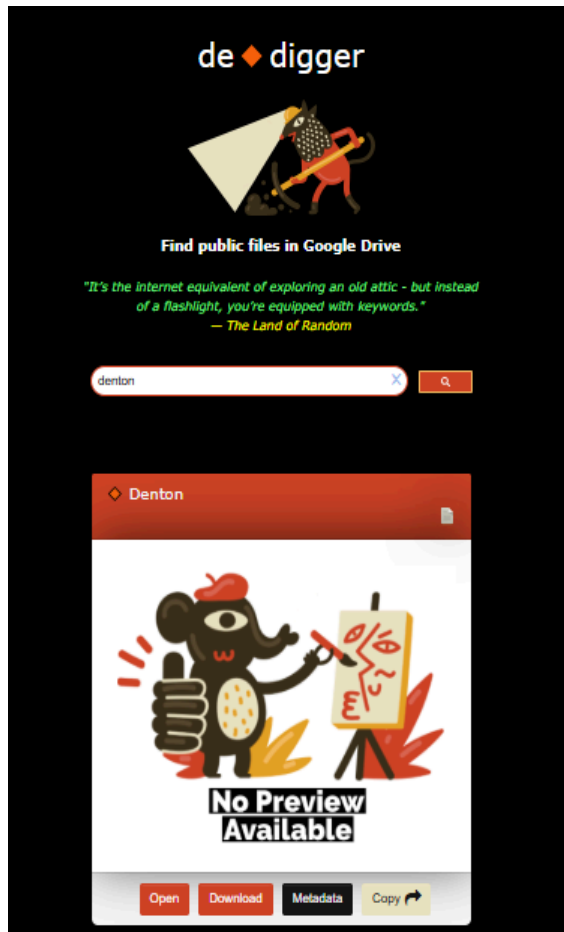
Domain Name	Creation Date	Registrar
alienindustries.us	2023-06-21	DOMAIN.COM, LLC
investigativeholdings.us	2020-07-15	NAMESILO, LLC
investigativepartner.com	2005-11-17	TUCOWS DOMAINS INC.
lancef.com	2005-12-01	TUCOWS DOMAINS INC.
marcusdoyle.com	2005-12-01	TUCOWS DOMAINS INC.
probeinfo.us	2019-10-11	NAMESILO, LLC
vcrinvestigation.com	2005-11-17	TUCOWS DOMAINS INC.
veracityresearchcompany.com	2005-11-17	TUCOWS DOMAINS INC.
vrc-inv.com	2005-12-01	TUCOWS DOMAINS INC.
vrcfightsfraud.com	2005-11-17	TUCOWS DOMAINS INC.
vrcinv.com	2005-12-01	TUCOWS DOMAINS INC.
vrcinvestigations.us	2007-08-12	NAMESILO, LLC

Others:

- <https://whois.domaintools.com/>
- <https://who.is/>
- <https://lookup.icann.org/en>
- <https://www.namecheap.com/>
- <https://www.whoxy.com/>

DeDigger:

DeDigger allows you to search for public/exposed google drive files and folders.



OTHER RESOURCES:

Open Sanctions:

<https://www.opensanctions.org/>

Europe E-Justice Portal:

https://e-justice.europa.eu/106/EN/business_registers_in_eu_countries?source=post_page-----b9ebc4ca1ace-----

Journalist Database:

<https://offshoreleaks.icij.org/>

List of Entity Types by Country:

https://en.wikipedia.org/wiki/List_of_legal_entity_types_by_country?source=post_page-----b9ebc4ca1ace-----

SEC Search:

<https://www.sec.gov/search-filings>

MSB Search:

https://www.fincen.gov/msb-state-selector?source=post_page-----b9ebc4ca1ace-----

Start.me:

https://start.me/p/rxeRqr/aml-toolbox?embed=1&source=post_page-----b9ebc4ca1ace-----