

## **ARTEMIS GAS, INC Penetration Test Phase 1: Reconnaissance**

Nathan Tendido

Cybersecurity Career Track, Springboard

Penetration Test Capstone

August 13, 2023

## Phase 1 Introduction

In order to conduct a thorough penetration test and at the request of the client, ARTEMIS GAS, INC, penetration test activities will be performed from an external perspective. Contextual information should not be provided by the client to the tester at any point. Information used for testing activities will be solely based on intelligence gathered through publicly available information. By using only publicly available information, the tester is able to build a perspective similar to a potential external threat actor.

### Objective

- Build a robust external perspective profile of ARTEMIS GAS, INC's business structure, processes, employees, network, and technology stack using only publicly available information

OSINT Testing tools and techniques to be used are:

1. [Google & Google Dorks](#) (*Search Engine and Advanced Techniques*)
2. [theHarvester](#) (*Automated OSINT Frameworks*)
3. [Recon-ng](#) (*Automated OSINT Frameworks*)
4. [Maltego](#) (*Link Analysis and Data Visualization*)
5. [Business Info Sources: OpenCorporates, D&B, CorporationWiki](#) (*Domain and Web Intelligence*)
6. [Social Media Sources: Facebook, Instagram](#) (*Online Presence and Social Media*)
7. [Employment Resources: LinkedIn, Glassdoor](#) (*Online Presence and Social Media*)
8. [VoilaNorbert](#) (*Email and Contact Gathering*)
9. [Shodan](#) (*Internet Scanning and Enumeration*)
10. [SecurityTrails by Recorded Future](#) (*Internet Scanning and Enumeration*)
11. [Builtwith](#) (*Internet Scanning and Enumeration*)
12. [PassiveDNS by Mnemonic](#) (*DNS and Domain*)
13. [DNSDumpster](#) (*DNS and Domain*)
14. [DNSlytics](#) (*DNS and Domain*)

## Google & Google Dorks

### Search Engine and Advanced Search Techniques

Source	<ul style="list-style-type: none"> <li>• <a href="https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06">https://gist.github.com/sundowndev/283efaddbcf896ab405488330d1bbc06</a></li> <li>• <a href="https://hackr.io/blog/google-dorks-cheat-sheet">https://hackr.io/blog/google-dorks-cheat-sheet</a></li> <li>• <a href="https://www.exploit-db.com/google-hacking-database">https://www.exploit-db.com/google-hacking-database</a></li> </ul>
Objective	<p>Perform basic searches as a starting point, and then use Google Dorking techniques to find additional hidden relevant information which is typically hidden in code, scripts, filenames, headers, metadata, etc.</p> <p>Care should be taken as to not access legally restricted or private information without explicit and documented approved permission.</p>
Required Inputs	<p>Company name, other related parameters.</p> <p>Google Dorking requires specific parameters included with search query.</p>

## theHarvester

### Automated OSINT Frameworks

Source	<ul style="list-style-type: none"> <li>• <a href="https://www.kali.org/tools/theharvester/">https://www.kali.org/tools/theharvester/</a></li> <li>• <a href="https://github.com/laramies/theHarvester">https://github.com/laramies/theHarvester</a></li> </ul>
Objective	Perform an automated gathering of email addresses, subdomains, and virtual hosts from online sources.
Required Inputs	Domain OR Company name

```

└─(kali㉿kali)-[~]
$ theHarvester -d priceline.com -b google -l 20
*****
*     [ - ] [ - ] \ ^ / [ - ] [ F V E X ] [ - ] [ - ]
*   [ - ] [ ] [ ] / [ - ] [ - ] [ - ] [ - ] [ - ]
*     [ - ] [ - ] [ ] [ - ] [ ] [ - ] [ - ] [ - ]
*****
* theHarvester 3.2.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[*] Target: priceline.com
      Searching 0 results.
[*] Searching Google.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 1
-----
www.priceline.com:151.101.66.186, 151.101.130.186, 151.101.194.186, 151.101.2.186

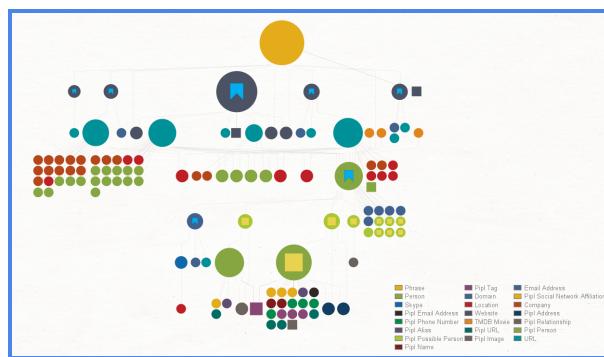
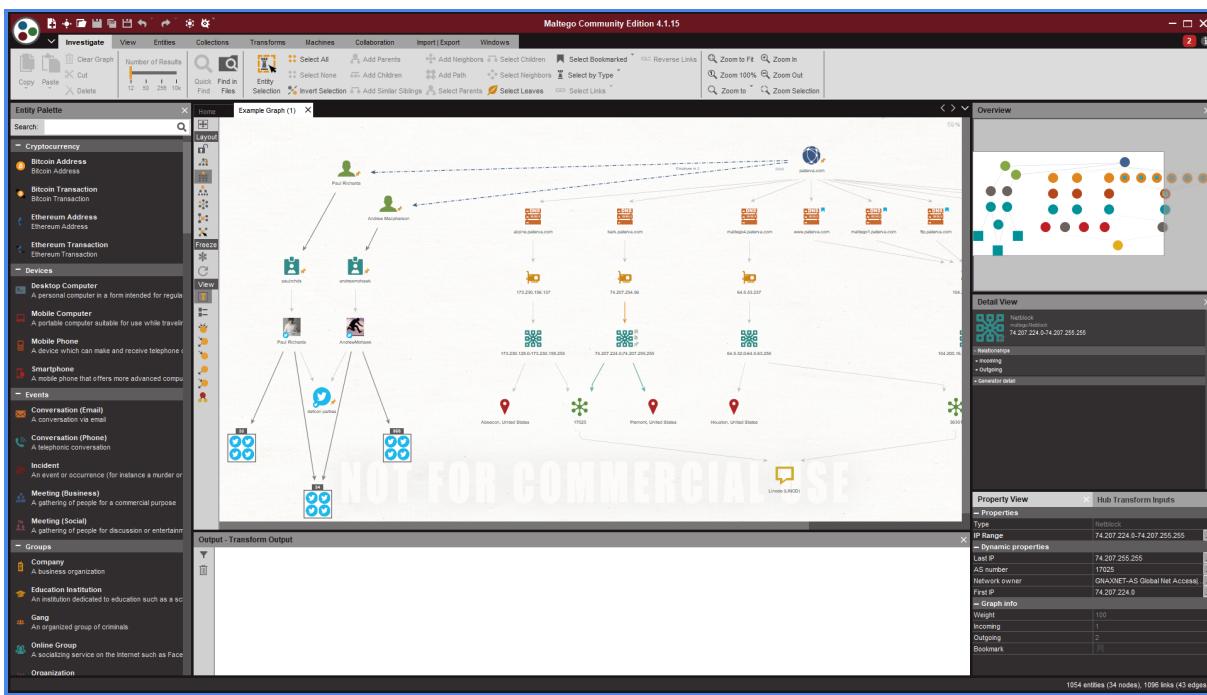
```



## Maltego

### Link Analysis and Data Visualization

Source	<ul style="list-style-type: none"> <li><a href="https://www.maltego.com/">https://www.maltego.com/</a></li> <li><a href="https://www.kali.org/tools/maltego/">https://www.kali.org/tools/maltego/</a></li> </ul>
Objective	Create a visualization to identify, map, and understand the target's online profile and relationship between public links.
Required Inputs	Domain name should be used for start, and additional queries can be run or manually added with other information gathered during Phase 1 (such as officer names, email addresses, subdomains, IP addresses, etc)



## Business Info Sources (OpenCorporates, D&B, CorporationWiki)

### Domain and Web Intelligence

Source	<ul style="list-style-type: none"> <li><a href="https://opencorporates.com/">https://opencorporates.com/</a></li> <li><a href="https://www.dnb.com/duns-number/lookup.html">https://www.dnb.com/duns-number/lookup.html</a></li> <li><a href="https://www.corporationwiki.com/">https://www.corporationwiki.com/</a></li> </ul>
Objective	Gather domain and business information, including ownership, financial, affiliate, officer, significant events, etc. for use as input in Phase 1 tools and target gathering
Required Inputs	Business name, entity name/s, officer names

**opencorporates**  
The Open Database Of The Corporate World

SEARCH Twitter Facebook LinkedIn Log in/Sign up

**Companies**  **Officers**

**Artemis Oil & Gas LLC**

Company Number 0803453822  
Status In Existence  
Incorporation Date 24 October 2019 (almost 4 years ago)  
Company Type Domestic Limited Liability Company (LLC)  
Jurisdiction Texas (US)  
Registered Address 1415 23RD ST  
CANYON  
79015-5323  
TX  
USA  
Alternative Names Artemis Oil & Gas LLC (trading name, 2019-10-25 -)  
Agent Name Natalie Bright  
Agent Address 1415 23rd Street, Canyon, TX, 79015, USA  
Directors / Officers 3 officers available, please log in to see this data  
Registry Page Please log in for link to primary source

Recent filings for Artemis Oil & Gas LLC

31 Dec 2022 PUBLIC INFORMATION REPORT (PIR)  
31 Dec 2021 PUBLIC INFORMATION REPORT (PIR)  
31 Dec 2020 PUBLIC INFORMATION REPORT (PIR)  
24 Oct 2019 CERTIFICATE OF FORMATION

Source: Texas Secretary of State, <https://direct.sos.state.tx.us/help/#...>, 29 Apr 2023

Dun & Bradstreet  
D-U-N-S® Number Lookup

Look up a partner company or find your company's D-U-N-S Number.

Search For Other company

Business Name Business Phone  
Legal Business Name\* ARTEMIS O&G

Name & Suffix Street Suite  
City & Zip-Code City Zip Code

State & Country\* Texas U.S.  
Search

I Found Results

See your company listed here? You can claim your D-U-N-S Number or update your company information. If you don't see your company's name in the search results, search by name or request a new D-U-N-S Number by filling out the box at the bottom of this screen.

ARTEMIS OIL & GAS LLC Overview

Artemis Oil & Gas LLC filed as a Domestic Limited Liability Company (LLC) in the State of Texas on Thursday, October 24, 2019 and is approximately 4 years old, as recorded in documents filed with Texas Secretary of State.

Learn More D&B Reports Available for Artemis Oil & Gas LLC Sponsored

Network Visualizer

## Social Media Sources (Facebook, Instagram)

### Online Presence and Social Media

Source	<ul style="list-style-type: none"> <li>• <a href="https://www.facebook.com/">https://www.facebook.com/</a></li> <li>• <a href="https://www.instagram.com/">https://www.instagram.com/</a></li> </ul>
Objective	Gather information on target's online presence on social media for use in target building and social engineering.
Required Inputs	Company name, officer name/s

## Employment Sources (LinkedIn, Glassdoor)

Online Presence and Social Media

Source	<ul style="list-style-type: none"> <li>• <a href="https://www.linkedin.com/">https://www.linkedin.com/</a></li> <li>• <a href="https://www.glassdoor.com/">https://www.glassdoor.com/</a></li> </ul>
Objective	Gather information on target's online presence on social media for use in target building and social engineering.
Required Inputs	Company name, officer name/s

## VoilaNorbert

### Email and Contact Information Gathering

Source	<ul style="list-style-type: none"><li>• <a href="https://www.voilanorbert.com/">https://www.voilanorbert.com/</a></li></ul>
Objective	Gather email addresses for target building and social engineering.
Required Inputs	Target name, known email address, or domain name

The screenshot shows the VoilaNorbert web application interface. On the left, there's a sidebar with navigation links: 'PROSPECTING' (selected), 'Manual', 'Bulk', 'CONTACTS', and 'API'. The main area has a search bar at the top with fields for 'Person name' and 'Domain.com'. Below the search bar, there's a green button labeled 'GO AHEAD, NORBERT!' and a link to 'Add 6 contacts to a list'. The main content area displays a list of contacts with their names, companies, and email addresses:

- Travis Kalanick Uber travis@uber.com
- Michael Arrington Techcrunch michael@techcrunch.com
- Larry Page Google larry.page@google.com
- Tim Cook Apple tcook@apple.com
- John Collison Stripe john.collison@stripe.com
- Ev Williams Medium ev@medium.com

Each contact entry includes a small profile picture, the contact's name, their company, and their email address. To the right of each entry are two circular icons: one with an envelope and another with a plus sign, likely for messaging or adding to a list. At the bottom right of the main area is a help icon (a question mark inside a circle).

## Shodan

### Internet Scanning and Enumeration

Source	<ul style="list-style-type: none"> <li><a href="https://www.shodan.io/">https://www.shodan.io/</a></li> </ul>
Objective	Identify internet-facing devices and services.
Required Inputs	Known IP address

The screenshot shows the Shodan search results for the IP address 34.102.136.180. The top navigation bar includes links for SHODAN, Explore, Pricing, and a search bar. Below the search bar is a map of the Kansas City area with the IP address highlighted. The main content area displays the following information:

**General Information**

Hostnames	180.136.102.34.bc.googleusercontent.com
Domains	GOOGLEUSERCONTENT.COM
Cloud Provider	Google
Cloud Region	global
Country	United States
City	Kansas City
Organization	Google LLC
ISP	Google LLC
ASN	AS396982

**Open Ports**

Open ports: 53, 80, 111, 443, 5432

**OpenResty**

```

HTTP/1.1 200 OK
Server: openresty
Date: Sun, 13 Aug 2023 18:58:00 GMT
Content-Type: text/html
Content-Length: 2930
Last-Modified: Sat, 12 Aug 2023 20:12:29 GMT
ETag: "64d7e7ad-b72"
X-AdBlock-Key: MFwwDQYJKoZIhvNAQEBBQADSwAwSAJBARDmzcpTevQqklnh6dJuX/N/HN+GxrruAKztliiC86+ewQ0msW1W8psOFL/000zklqsCaewAAQ_1w5V0di28J19HV3MQRA/nMpx427/1/kDFi8IhDn7KBAGSMgYRhCVj2IPMwHdBqUzQ
Cache-Control: no-cache
X-Content-Type-Options: nosniff
Set-Cookie: system=PW;Path=/;Max-Age=86400;
Set-Cookie: cof_ipaddr=224.211.186.214;Path=/;Max-Age=86400;
Set-Cookie: country=US;Path=/;Max-Age=86400;
Set-Cookie: city="";Path=/;Max-Age=86400;
Set-Cookie: traffic_target=gd;Path=/;Max-Age=86400;
Accept-Ranges: bytes
Via: 1.1 google

```

## SecurityTrails by Recorded Future

Internet Scanning and Enumeration

Source	• <a href="https://securitytrails.com/">https://securitytrails.com/</a>
Objective	Gather information on historical domain and IP information.
Required Inputs	Known domain name or IP address

The screenshot shows the SecurityTrails interface for the domain `artemisenergypartners.com`. The left sidebar has tabs for DOMAIN, DNS Records (selected), Historical Data, and Subdomains (with 2 results). A blue button says "Sign up for an API key now!" and "Sign up". The main content area displays DNS records as of Aug 13, 2023:

- A records:** Google LLC (35.192.73.176) [218]
- AAAA records:** NO RECORDS
- MX records:** Microsoft Corporation (1 record: artemisenergypartners-com.mail.protection.outlook.com)
- NS records:** Cloudflare, Inc., ns72.worldnic.com, ns71.worldnic.com
- SOA records:** ttl: 10800, email: namehost.worldnic.com [2,475,932]
- TXT:**

```
v=spf1 include:spf.protection.outlook.com ip4:10.16
include:spf.protection.outlook.com ~all ip4:10.168.2
include:spf.protection.outlook.com ~all
include:_spf.prod.hydra.sophos.com -all
sophos-domain-
```

## Builtwith

### Internet Scanning and Enumeration

Source	<ul style="list-style-type: none"> <li><a href="https://builtwith.com/">https://builtwith.com/</a></li> </ul>
Objective	Analyze web technologies in use for a domain and identify technology stacks, frameworks, plugins, and tools used.
Required Inputs	Domain name or IP address

The screenshot shows the Builtwith interface for the domain `artemisenergypartners.com`. The top navigation bar includes links for Tools, Features, Plans, Customers, Resources, and a search bar with the query `artemisenergypartners.com` and a **Lookup** button. Below the navigation is a breadcrumb trail: Home / artemisenergypartners.com Technology Profile.

# ARTEMISENERGYPARTNERS.COM

The main content area features tabs for Technology Profile (selected), Detailed Technology Profile, Meta Profile, Relationship, Redirect, Recommendations, and Company. The Technology Profile tab displays the following sections:

- Widgets**: Includes a section for **Pexels** (free stock photos, royalty free images & videos) and **Contact Form 7** (specifically designed for WordPress blogs).
- Font Awesome**: Includes a section for **Wordpress Plugins** (tools to extend WordPress functionality).
- Sitelinks Search Box**: Includes a section for **RankMath** (a plugin for optimizing WordPress sites).
- Profile Details**: Shows last detection on July 20, 2023, and lists 39 technologies found on the page, with 6 removed since December 2021. It also includes a "Create Notification" button for tracking new technologies.
- Recent Lookups**: A sidebar listing various websites such as acpi.com.br, molo13.it, crawlly.com.br, adcc.com.cn, cooperweston.co.uk, apnijaidad.com.pk, keralatravelcentre.com, watersplashnet.com, driesenberg.de, erobito.com, dndoog.com, kaettelueckenhaus.de, brightweb.com, equibase.com, rinse.vc, envirse.com, studiohikari.com.br, desibees.com, fpsi.org, multicraft.world, hotelaltefeuerwache.de, xemico.com, nublemate.com, sempreavista.com.br, wmoi.com, margraphics.com, physifox.com, mokstor.com, roobot.de, montrealimmosvip.com, acpf.com.br, natcglobal.com, agrobasic.ro, daxiron.com, ipcom.be, contadorinc.co.za, referin.com, ruteam.ru, e-bikes.io, xn--vj1b84kq5kd2g.kr, treinal.com, acpilates.com.br.

## PassiveDNS by Mnemonic

DNS and Domain Information

Source	<ul style="list-style-type: none"><li>• <a href="https://passivedns.mnemonic.no/">https://passivedns.mnemonic.no/</a></li></ul>
Objective	Gather passive DNS data to build DNS history and resolution profile.
Required Inputs	Domain name or IP address

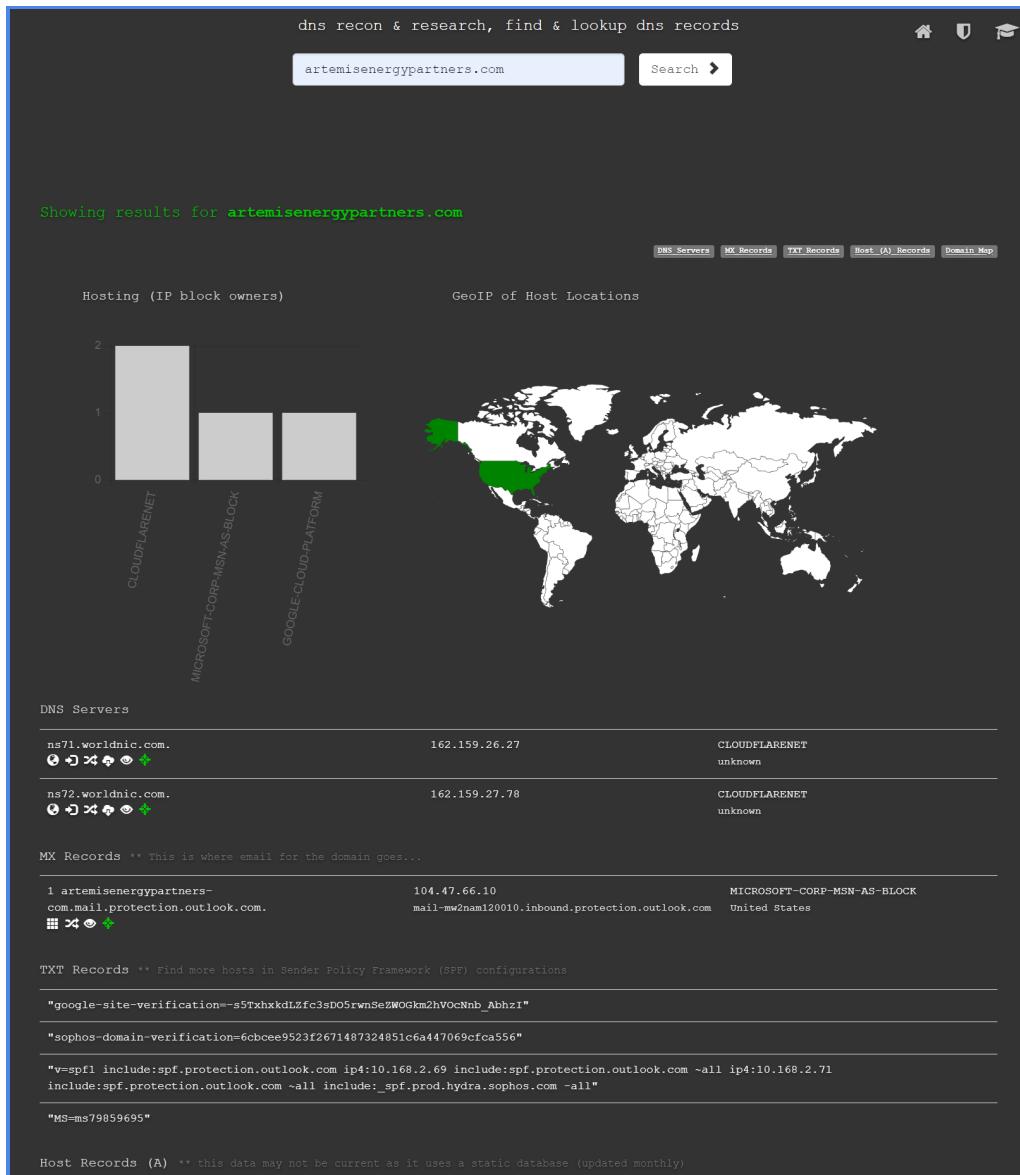
The screenshot shows the PassiveDNS by Mnemonic web application. At the top, there is a large logo with the words "PASSIVE" and "DNS" in white and orange. Below the logo is a search bar containing the query "artemisenergypartners.com". The main content area displays a table of DNS records. The columns are labeled: Record type, Query, Answer, First seen, Last seen ↓, # times, and TTL. A single record is shown: an "a" record for "artemisenergypartners.com" with the answer "35.192.73.176", first seen on 2023-03-21 12:30, last seen on 2023-08-08 03:43, 7 occurrences, and a TTL of 7200. To the right of the table is a vertical sidebar titled "History" which shows a single entry for "artemisenergypartners.com" from 15 seconds ago. At the bottom of the page, there are navigation links for "Showing: 25", "1-1 of 1", and "PREVIOUS NEXT".

Record type	Query	Answer	First seen	Last seen ↓	# times	TTL
a	<a href="#">artemisenergypartners.com</a>	35.192.73.176	2023-03-21 12:30	2023-08-08 03:43	7	7200

## DNSDumpster

### DNS and Domain Information

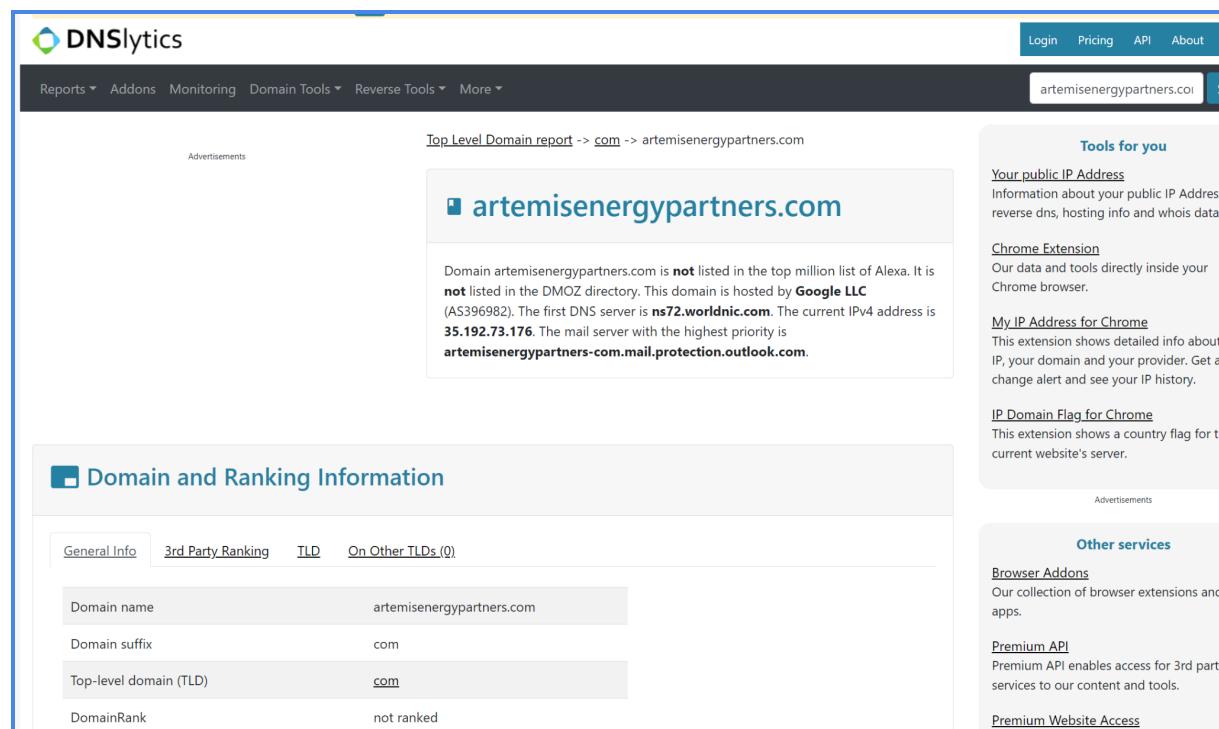
Source	<ul style="list-style-type: none"> <li><a href="https://dnsdumpster.com/">https://dnsdumpster.com/</a></li> </ul>
Objective	Gather DNS domain and subdomain information associated with the target domain.
Required Inputs	Domain name



## DNSlytics

### DNS and Domain Information

Source	• <a href="https://dnslytics.com/">https://dnslytics.com/</a>
Objective	Gather DNS and domain information.
Required Inputs	Domain name, IPv4, or IPv6 address



The screenshot shows the DNSlytics interface. At the top, there's a navigation bar with links for Reports, Addons, Monitoring, Domain Tools, Reverse Tools, More, Login, Pricing, API, and About. A search bar is also present. The main content area displays domain analysis for 'artemisenergypartners.com'. It includes a summary section with a blue icon, the domain name, and a brief description stating it's not listed in Alexa or DMOZ, hosted by Google LLC, and has an IPv4 address of 35.192.73.176. Below this is a 'Domain and Ranking Information' section with tabs for General Info, 3rd Party Ranking, TLD, and On Other TLDs (0). The General Info tab is selected, showing details like Domain name (artemisenergypartners.com), Domain suffix (com), Top-level domain (TLD) (com), and DomainRank (not ranked). To the right, there are 'Tools for you' sections: 'Your public IP Address' (information about public IP, reverse DNS, hosting info, WHOIS data), 'Chrome Extension' (data and tools directly in Chrome browser), 'My IP Address for Chrome' (extension for detailed IP info), and 'IP Domain Flag for Chrome' (extension for country flag of current server). There are also 'Other services' sections for Browser Addons (collection of browser extensions and apps), Premium API (access for 3rd party services), and Premium Website Access.

## Phase 1 Conclusion

Activities conducted during Phase 1 are not expected to have any major impact on client's business activities. The focus during this phase is to build a contextual profile using publicly available resources with information to be used in later testing phases.

### Preparer Approval

Signature:

Name:

Date:

### Client Approval

Signature:

Name:

Date: