dns recon & research, find & lookup dns records
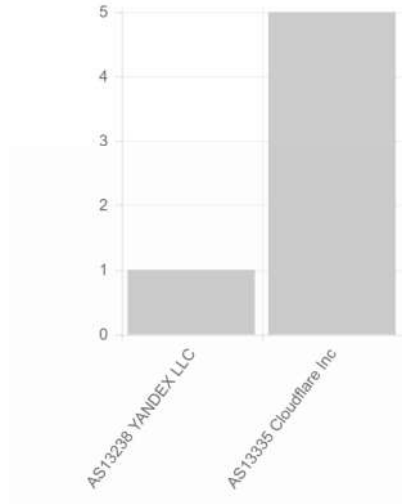
    exampledomain.com

    Search ❯

Showing results for **seodima.com**

[DNS Servers] [MX Records] [TXT Records] [Host (A) Records] [Domain Map]

Hosting (IP block owners)

GeoIP of Host Locations

DNS Servers

abby.ns.cloudflare.com. ⊞ (https://api.hackertarget.com/reverseiplookup/?q=173.245.58.100) 🌐 (https://api.hackertarget.com/httpheaders/?q=) ⤭ (https://api.hackertarget.com/mtr/?q=173.245.58.100) ☁ (https://api.hackertarget.com/findshareddns/?q=abby.ns.cloudflare.com.)	173.245.58.100 abby.ns.cloudflare.com	AS13335 Cloudflare Inc United States
sid.ns.cloudflare.com. ⊞ (https://api.hackertarget.com/reverseiplookup/?q=173.245.59.143) 🌐 (https://api.hackertarget.com/httpheaders/?q=) ⤭ (https://api.hackertarget.com/mtr/?q=173.245.59.143) ☁ (https://api.hackertarget.com/findshareddns/?q=sid.ns.cloudflare.com.)	173.245.59.143 sid.ns.cloudflare.com	AS13335 Cloudflare Inc United States

MX Records ** This is where email for the domain goes...

```
10 mx.yandex.net.                                                                      213.180.193.89   AS13238
⊞ (https://api.hackertarget.com/reverseiplookup/?q=213.180.193.89) 🌐 (https://api.hackertarget.com/httpheaders/?   mx.yandex.ru     YANDEX
q=http://) ⤭ (https://api.hackertarget.com/mtr/?q=213.180.193.89)                                       LLC
                                                                                                        Russian
                                                                                                        Federation
```

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"v=spf1 redirect=_spf.yandex.net"
```

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

```
seodima.com                                                                            104.27.152.23    AS13335
⊞ (https://api.hackertarget.com/reverseiplookup/?q=104.27.152.23) 🌐 (https://api.hackertarget.com/httpheaders/?   Cloudflare
q=http://seodima.com) ⤭ (https://api.hackertarget.com/mtr/?q=104.27.152.23)    cloudflare-nginx         Inc
```

```
seodima.com                                                                            104.27.152.23    AS13335
⊞ (https://api.hackertarget.com/reverseiplookup/?q=104.27.152.23) 🌐 (https://api.hackertarget.com/httpheaders/?   Cloudflare
q=http://seodima.com) ⤭ (https://api.hackertarget.com/mtr/?q=104.27.152.23)    cloudflare-nginx         Inc
```

```
seodima.com                                                                            104.27.153.23    AS13335
⊞ (https://api.hackertarget.com/reverseiplookup/?q=104.27.153.23) 🌐 (https://api.hackertarget.com/httpheaders/?   Cloudflare
q=http://seodima.com) ⤭ (https://api.hackertarget.com/mtr/?q=104.27.153.23)    cloudflare-nginx         Inc
```

⊕ Download .xlsx of Hosts   (https://dnsdumpster.com/static/xls/seodima.com-201710140932.xlsx)

Mapping the domain ** click for full size image
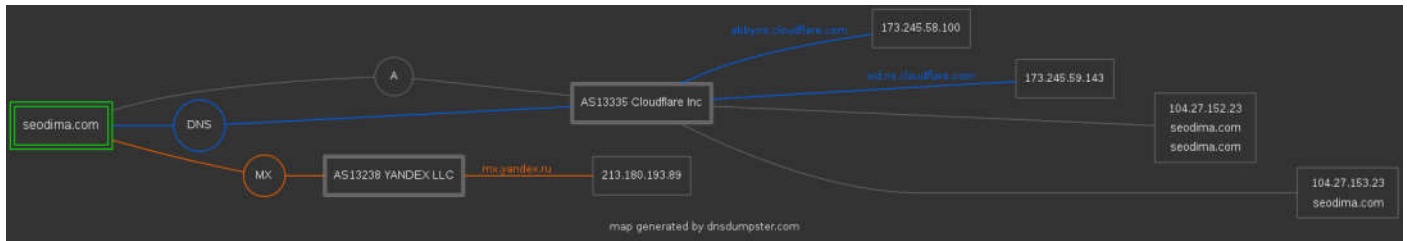
(/static/map/seodima.com.png)

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a HackerTarget.com (https://hackertarget.com/) project

Head over to HackerTarget.com (https://hackertarget.com/) for access to the domain profiler tool. Enumerate a domain and pull back an XLS with up to 40K subdomains. Get the edge whether you are chasing bug bounties , red teaming a new target or mapping your attack surface .

Membership includes **9** vulnerabiltiy scanning tools.
Trusted tools hosted for remote easy access.

⌄

🗑

Map an organizations attack surface with a virtual *dumpster dive** of the DNS records associated with the target organization.

*DUMPSTER DIVING: The practice of sifting refuse from an office or technical installation to extract confidential data, especially security-compromising information.
Dictionary.com

⌄

⚙

More than a simple DNS lookup (https://hackertarget.com/dns-lookup/) this tool will discover those hard to find sub-domains and web hosts. No brute force of common sub-domains is undertaken as is common practice for many DNS recon tools. The search relies on data from search engines and the excellent scans.io (https://scans.io) research project.

Receive updates by following @hackertarget (https://twitter.com/hackertarget) on Twitter
or subscribe to the low volume mailing list (http://eepurl.com/jDaVL).

this is a HackerTarget.com (https://hackertarget.com/) project