Example web query https://www.onyphe.io/

Example API query using ONYPHE CLI or curl

ONYPHE Free View Cheat Sheet

https://www.onyphe.io/docs/onyphe-query-language

Services & networks

Find exposed services on a domain

```
protocol:telnet domain:example.com
```

ONYPHE performs protocol detection on all scanned ports

Find open ports on an IP

```
ip:8.8.8.8
```

Click on the Overview tab to view open ports and protocols

Check for a specific open port on an IP

```
ip:8.8.8.8 port:443
```

using 'protocol:http' would list non-standard http(s)ports

Check for non-http services on a hostname

```
hostname:www2.example.com !protocol:http
```

Boolean AND is implied between filters. ! = NOT

Find exposed services with a web address

```
forward:www.example.com
```

URL scans inject 'forward' into the http host header

Passive DNS query of MX records

```
category:resolver type:mx domain:example.com
```

Queries to the ONYPHE resolver are totally passive

Search for threats by Autonomous System Number

```
category:threatlist asn:AS12389
```

Free categories are ctl, datascan (default), resolver, and threatlist

TLS & Certificates

Search within TLS certificates

```
subject.organization:NSA
```

Check out the asset json tab to see all collected data

Find TLS certs matching a fingerprint

```
fingerprint.sha256:"dfbd543...4e446d"
```

md5 and sha1 hashes also available

Search within Certificate Transparency Logs

```
category:ctl domain:cloudflare.com
```

CTL data is updated in real-time

Systems & devices

Search for operating systems by domain

```
os:windows domain:example.com
```

OS values: https://www.onyphe.io/docs/dorkpedia/os-list

Search for specific products on a domain

```
product:"Exchange Server" domain:example.com
```

Product list: https://www.onyphe.io/docs/dorkpedia/product-list

Full text search within service banners

```
data:"Microsoft Exchange IMAP4"
```

Searches within service responses for all words in the phrase

Search for a specific OS distribution on a domain

```
osdistribution:debian domain:redhat.com
```

Product list: https://www.onyphe.io/docs/dorkpedia/product-list

Search for a specific product version

```
product:"MySQL" productversion:"5.5.20"
```

Wildcard searches are possible with enterprise-level licenses

Web apps

Find http application components with a TLD

```
app.http.component.product:PHP tld:com
```

Click the Software tab to view all asset app components

Search for backlinks to a domain

```
app.extract.domain:t.me !domain:t.me
```

app.extract data is extracted from http responses

Full-text search within HTTP titles

```
app.http.title:camera !port:443 !port:80
```

HTML keywords, description and copyright metadata also indexed

Find all assets with the same HTTP headers

```
app.http.headermd5:"1c285aa85b3...dbed10"
```

Use the Analytics tab to quickly pivot to identical services

Full-text search within HTTP keywords

```
app.http.keywords:ASM
```

Add more filters by clicking on asset results

Geolocation

Search for assets by country

```
$ onyphe -search 'country:uk'
```

CLI documentation : https://www.onyphe.io/docs/cli/installation

```
$ curl -H 'Content-Type: application/json' -H 'Authorization: bearer <APItoken>' -XGET 'https://www.onyphe.io/api/v2/search/?q=country:fr'
```

Geolocate assets in a domain using CLI & OPP

```
$ onyphe -search 'domain:example.com | fields ip,port,location | output'
```

Onyphe Processing Pipeline https://www.onyphe.io/docs/cli/opp

Hosting organization and continent by domain

```
$ onyphe -search 'domain:akamai.com | fields ip,organization,geolocus.continentname | output'
```

onyphe -h displays help about command line and APIs

Cool stuff

Everything we know about a hostname

```
$ onyphe -summary hostname www.apple.com
```

Summary API can also answer queries about domains and IPs

Unique results only, and add a counter

```
$ onyphe -search 'app.http.component.productvendor:"Cobalt Strike" country:nl | uniq domain | addcount'
```

Butterfly view license allows 10,000 results a month

More about ONYPHE

- Founded in 2017, ONYPHE scans the IPv4 address space, hostnames, URLs, IPv6, TLS certs and more.
- Our founder defined an ethical approach to scanning the Internet : https://www.onyphe.io/docs/write-ups/our-10-commandments-for-ethical-internet-scanning
- Enterprise views with vulnscan category detect over 50 CVEs on the CISA KEV catalog. Unlimited results & advanced queries.
- Cybersecurity Asset Attack Surface Management (CAASM) and Asset Discovery. Built by defenders for defenders.

https://www.onyphe.io/files/onyphecheatsheetfreeview.pdf