# CENSYS Quick Start Reference

censys.io

## What is Censys?

Censys is a publicly available search engine, similar to Shodan but unique in its own right, which scans the entire Internet for a limited number of services and enumerates discovered services by their banner responses, indexes that data and makes it searchable.

Censys stores the information in structured fields which can be queried specifically for enumerating data on hosts, services and (in particular) web certificates.

Be sure to use the **'Raw Data'** option on any discovered host to see all of the data types Censys has stored.

Censys also indexes WHOIS data which can be viewed from the same menu under **"Raw WHOIS"**.

## IP Addresses & Subnets

**Single IP Address** – Search for findings on single IP
Example: **52.179.197.205** *or* **ip:52.179.197.205**

**IP Subnet by CIDR** – Search across a specific CIDR
Example: **ip:52.179.197.0/24**

**IP Subnet by Range** – Search across a specific range
Example: **ip:[216.189.94.1 TO 216.189.94.32]**

**Hostname** – Search on result of a DNS "A" / host entry
Example: **a:panerabread.com**

**Mail Servers** – Search on DNS "MX" entries for domain
Example: **mx:panerabread.com**

**Port** – Find any instances of active services on a port
Example: **ports:21**

**Service** – Search for instances of specific services
Example: **protocols:"21/ftp"**

**Autonomous System Number (ASN)** – Search by ASN
Example: **autonomous_system.asn: 7018**

## Physical Location

**Country** – Search by country code
Example: **location.country_code:"US"**

**City** – Search by city name
Example: **location.city:Paris**

**State** – Search by state name
Example: **location.province:South Carolina**

**Zip Code** – Search by postal ZIP code
Example: **location.postal_code:92127**

**Geo : Latitude Range** – Search GPS coordinates - Latitude
Example: **location.latitude:[45.0 TO 59.0]**

**Geo : Longitude Range** – Search GPS coordinates - Longitude
Example: **location.longitude:[15.0 TO 18.5]**

## Operating Systems & Products

**Operating System** – Search by operating system type
Examples: **metadata.os:Windows**

**Product (Web Service)** – Search by known product name
Example: **443.https.get.metadata.product:nginx**

**Manufacturer** – Search for known manufacturers
Example: **metadata.manufacturer:"Huawei"**

**Microsoft SMBv1** – Search for instances of SMBv1
Example: **445.smb.banner.smbv1_support:true**

## Dates & Ranges

**Date: After** – Search for findings that appear after a date
Example: **updated_at:[2018-12-15 TO *]**

**Date: Before** – Search for findings that appear before a date
Example: **updated_at:[* TO 2018-12-31]**

**Date : Range** – Search for findings that appear within a range
Example: **updated_at:[2018-12-15 TO 2018-12-31]**

## Web Apps

**Page's Title** – Search for text in page's title
Example: **443.https.get.title:"Index of /ftp"**

**Page's HTML Body** – Search body of webpage for text string
Example: **443.https.get.body:"XML-RPC server accepts"**

**Web Technologies** – Search for specific web technologies
Example: **443.https.get.metadata.product: php**

**TLS Version** – Determine most recent version supported
Example: **443.https.tls.version:TLSv1.2**

**SSLv3** – Find instances of SSLv3
Example: **443.https.ssl_3.support:true**

**Expired Certificates** – Search for expired HTTPS certs
Example:
**443.https.tls.certificate.parsed.validity.end:[2018-12-31 TO *]**

**Self-Signed Certificates** – Search for expired HTTPS certs
Example:
**443.https.tls.certificate.parsed.signature.self_signed:true**

**Invalid Cert Signatures** – Find invalid cert signatures
Example:
**443.https.tls.certificate.parsed.signature.valid:false**

**Trusted Certs** – Determine trusted certs by browsers
Example: **443.https.tls.validation.browser_trusted**

**Heartbleed** – Find potential instances of Heartbleed vuln
Example:
**443.https.heartbleed.heartbleed_vulnerable:true**

## Tags

**A list of common tags that I've found useful:**
bacnet, database, DSL/cable modem, embedded, Heartbleed, industrial control system, known-private-key, modbus, mssql, mysql, network, oracle, postgres, printer, rdp, remote_display, raspberry pi, scada, smb, vnc

**A special thank you to the Censys team (@censysio) and the University of Michigan (@UMich) !!!**

**By Michael Holcomb (@mdholcomb)**