

Passive Reconnaissance with Digital Certificates

@mmar



- We are trying to find subdomains of a website that may be using the same digital certificate



Digital certificates are primarily used to ensure the security and authenticity of websites. They help to establish a secure connection between a user's browser and the website they are trying to access, by verifying that the website is legitimate and encrypting the data that is exchanged between the two parties.

Digital certificates can also be used to discover **subdomains of a website**. When a certificate is issued for a specific domain, it is typically issued for that domain and any of its subdomains. Therefore, by searching for certificates issued to a particular domain, it is possible to discover subdomains that are associated with that domain.

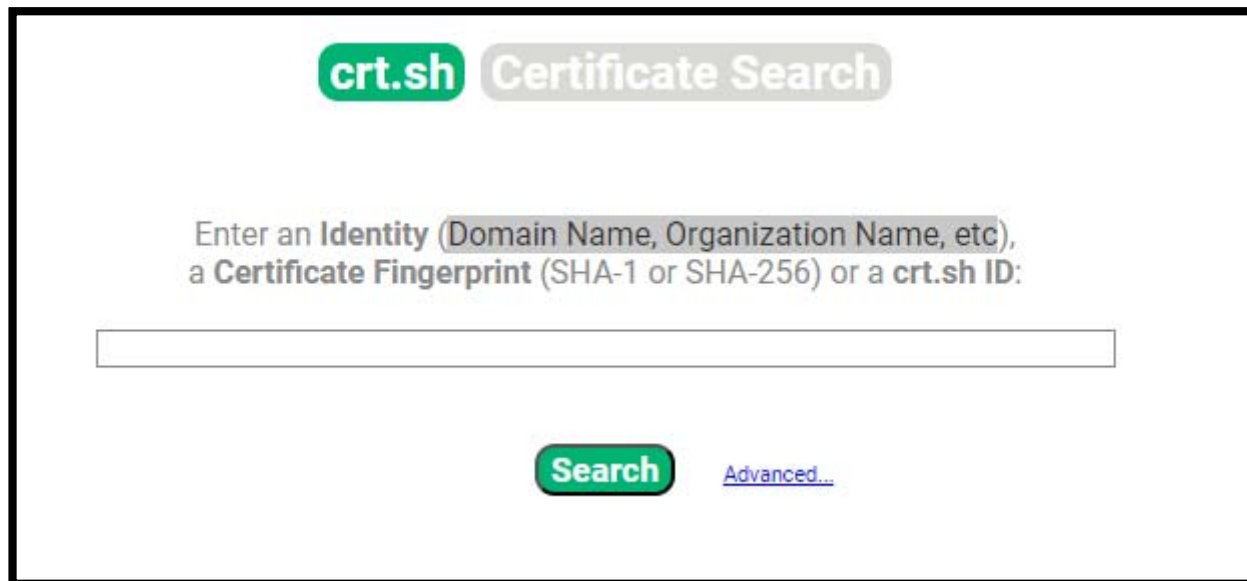


Digital Certs search engines

Crt.sh

- ❖ Allows searching with Domain Name, Organization Name, etc

<https://crt.sh/>

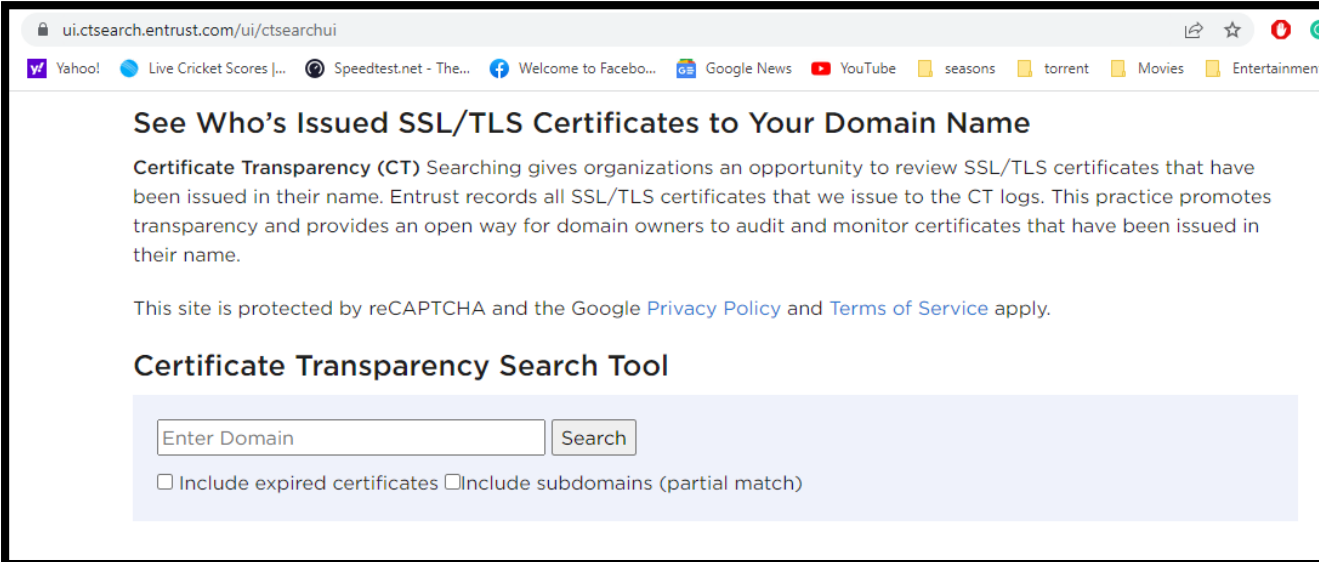


The screenshot shows the crt.sh Certificate Search interface. At the top, there is a green 'crt.sh' logo and a grey 'Certificate Search' button. Below this, the text reads: 'Enter an Identity (Domain Name, Organization Name, etc), a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:'. Underneath the text is a long, empty text input field. At the bottom of the form, there is a green 'Search' button and a blue link labeled 'Advanced...'.

Entrust cert search

- ❖ Allows searching for partial as well as expired certificates

<https://ui.ctsearch.entrust.com/ui/ctsearchui>



The screenshot shows a web browser window with the URL `ui.ctsearch.entrust.com/ui/ctsearchui`. The page title is "See Who's Issued SSL/TLS Certificates to Your Domain Name". Below the title, there is a paragraph explaining Certificate Transparency (CT) searching. A search tool is provided with a text input field labeled "Enter Domain", a "Search" button, and two checkboxes: "Include expired certificates" and "Include subdomains (partial match)".

See Who's Issued SSL/TLS Certificates to Your Domain Name

Certificate Transparency (CT) Searching gives organizations an opportunity to review SSL/TLS certificates that have been issued in their name. Entrust records all SSL/TLS certificates that we issue to the CT logs. This practice promotes transparency and provides an open way for domain owners to audit and monitor certificates that have been issued in their name.

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

Certificate Transparency Search Tool

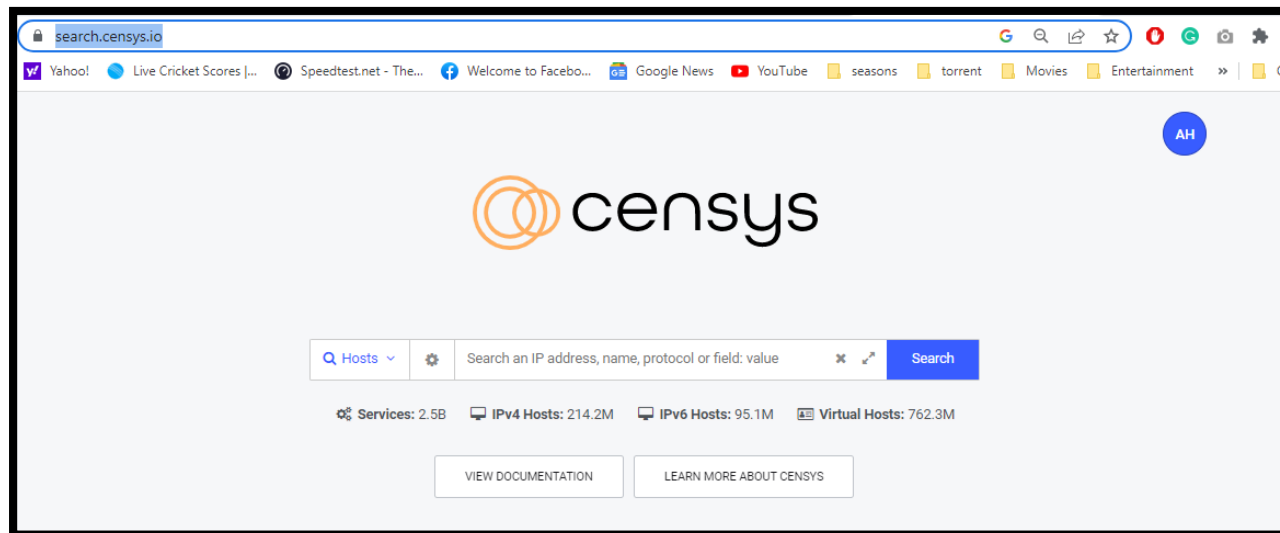
Enter Domain Search

Include expired certificates Include subdomains (partial match)

Censys

- ❖ Censys is a search engine for all internet connected devices and has a separate functionality to search digital certificates

<https://search.censys.io/>



DEMO



THANKS