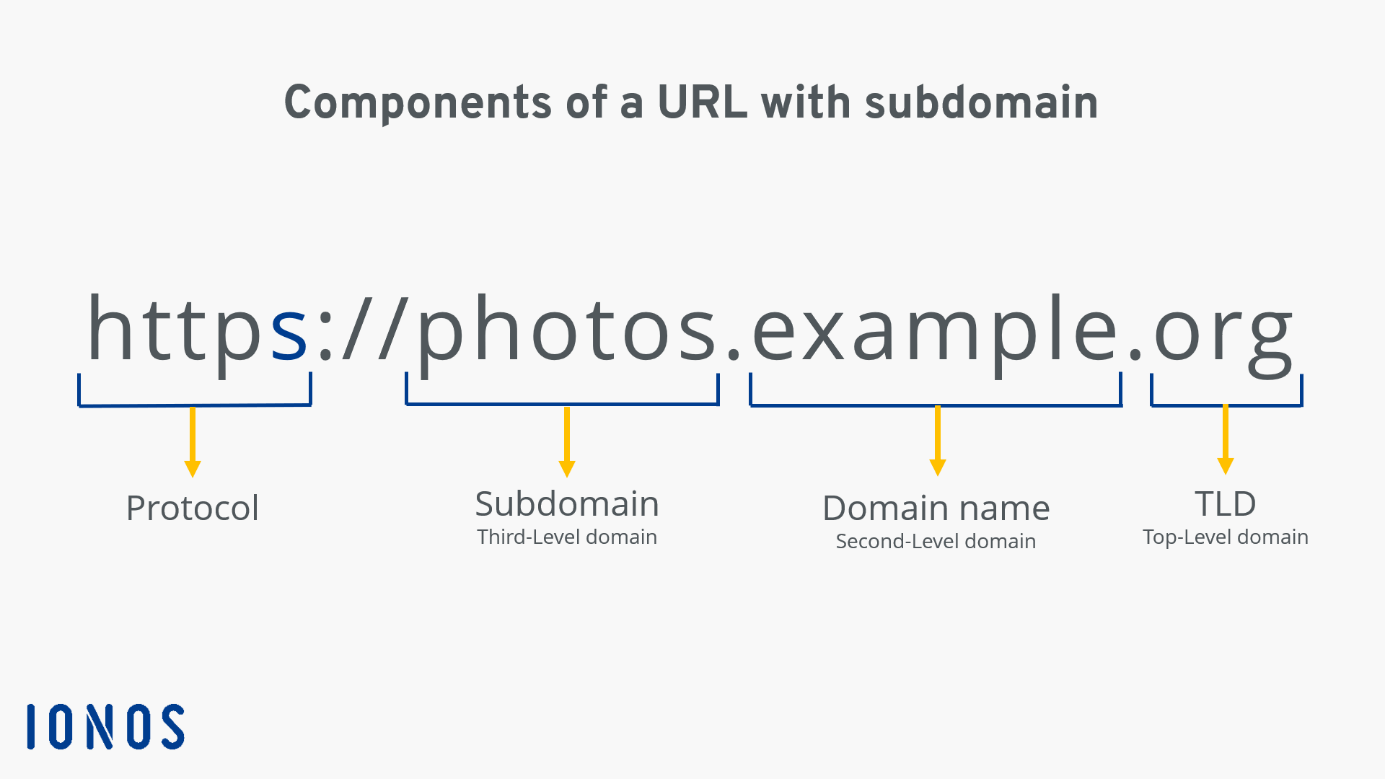
**Subdomains**

Subdomains can be thought of as a secondary component for a web URL

Or it can be thought of as a separate domain that is still apart of the main domain

For example, Wikipedia can have multiple subdomains such as uk.wikimedia, store.wikimedia, jobs.wikimedia, species.wikimedia, etc.

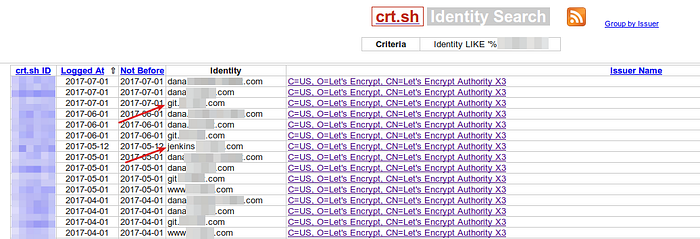


**How Does Subdomain Enumeration Work?**

It can be used to access hidden subdomains within a main domain, for example a website such as Google has a multitude of subdomains hidden from the public eye unless specified. With Subdomain Enumeration, you can uncover all these subdomains and use them to gather information, assess potential vulnerabilities and create a gateway for more sophisticated methods of attack.

**Certificate Transparency (CT)**

Certificate Transparency is a required project established by the Certificate Authority to post every SSL/TLS certificate onto a public log, usually concerning domain names, subdomains and email addresses. This can further help when searching for subdomains and hidden webpages/sites on a main domain



Tools such as ThreatCrowd, Crt.sh, and VirusTotal offer API tools to help further uncover subdomains and their respective IPs

**Project Plan**

As of right now, the plan for this Python project is to be able to scan either a DNS or IP address and resolve their subdomains as well as the IP to go along with those sub domains. This will also be used as a DNS resolver to convert IP addresses into a Domain Name. This project requires the usage of HTTP GET requests, DNS resolving, JSON parsing, and DNS 🡪 IP Address.

**HTTP GET Requests**

HTTP GET Requests are ways to receive and save data. Getting information such as JSON, XML and HTML requests, you can receive all this information from the server using the GET request. In Python you can fetch data from online API’s or websites using this request.

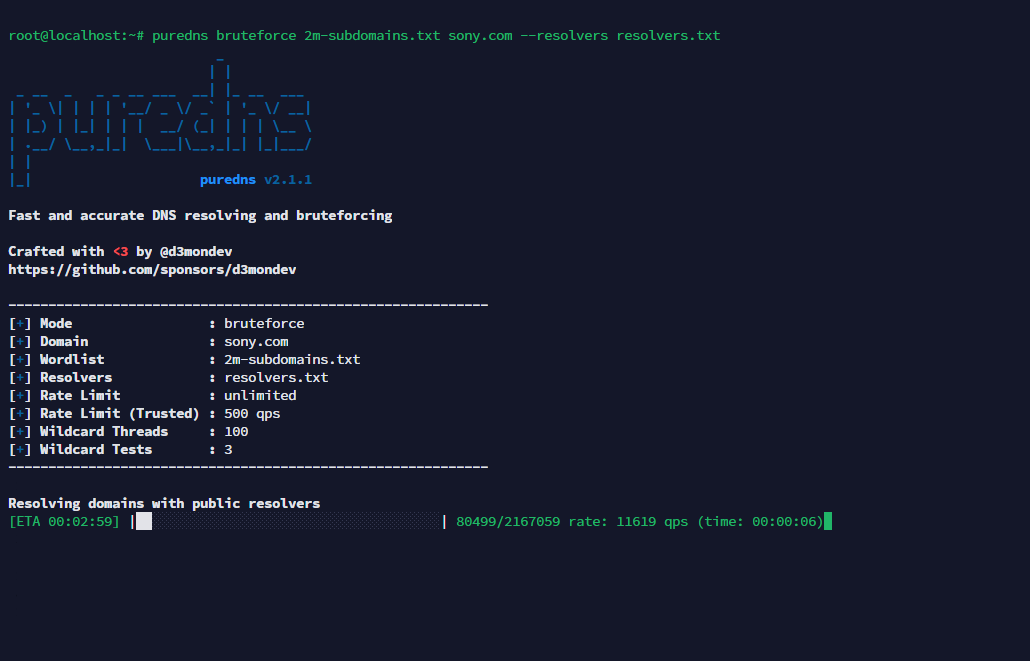
**Passive vs Active Enumeration**

Passive Subdomain Enumeration revolves around getting information without directly interacting with the specific target domain. Google Dork is a tool that can be used to do this.

Active Subdomain Enumeration is the exact opposite, requiring the user to directly interact with the domain using techniques such as brute-forcing subdomains, DNS requests, or using Certificate Transparency Logs. Subfinder is a tool that can be used to find this.

**Permuted Subdomain Enumeration**

Involves using a word list or large TXT file for potential subdomains by altering or adding terms onto a domain to have a chance of catching a subdomain. For example, if “api.example.com” is a known subdomain, a user might try “api-test.example.com” to check if that exists.



**Record Types**

For this project understanding Record Types such as A, AAAA, CNAME, MX, and TXT are crucial.

**A Record**

Maps a domain to an IPv4 Address

Example: claude.ai 🡪 160.79.104.10

**AAAA Record**

Maps a domain to an IPv6 Address

Example: claude.ai 🡪 2607:6bc0::10

**CNAME Record**

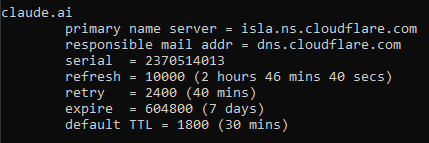
Allows multiple domain names to point to one singular domain

bar.example.com. 🡪 CNAME foo.example.com.

This would be the same as saying “*bar.example.com*” is an alias for the canonical name (CNAME) for “*foo.example.com*” meaning a client will request “*bar.example.com*” and the answer will be “*foo.example.com*”.

**MX Record**

Specifies mail servers responsible for accepting email for the domain



**DNS Queries and Lookups**

Used for resolving a DNS name it queries to either the main root server (recursive) to receive and answer or the current DNS server gives an answer based on its own knowledge (iteration). For example, a DNS query could be a client asking for any A records for a machine named Google.com, using either of the two ways, the root server or current DNS server will try its best to give an answer to the client.

**Current Standings and Future Plans**