DomainTools

DNSDB Scout

User Guide / Workflows

domaintools.com

Product Overview

DNSDB Scout

Investigative platform and API draws on 15+ years of current and historical passive DNS data that enables efficient DNS-based investigations in an intuitive UI.

Comprehensive passive DNS data of near real-time and historical global Internet infrastructure data. All observed questions and responses are included as well as all resource record types.

- 2TB DNS DATA COLLECTED DAILY
- 100+ BILLION DNS RECORDS
- 800k+ OBSERVATIONS PER SECOND
- 1GB/SEC REAL-TIME STREAMING DATA

DomainTools

Getting Started

01 Account Activation

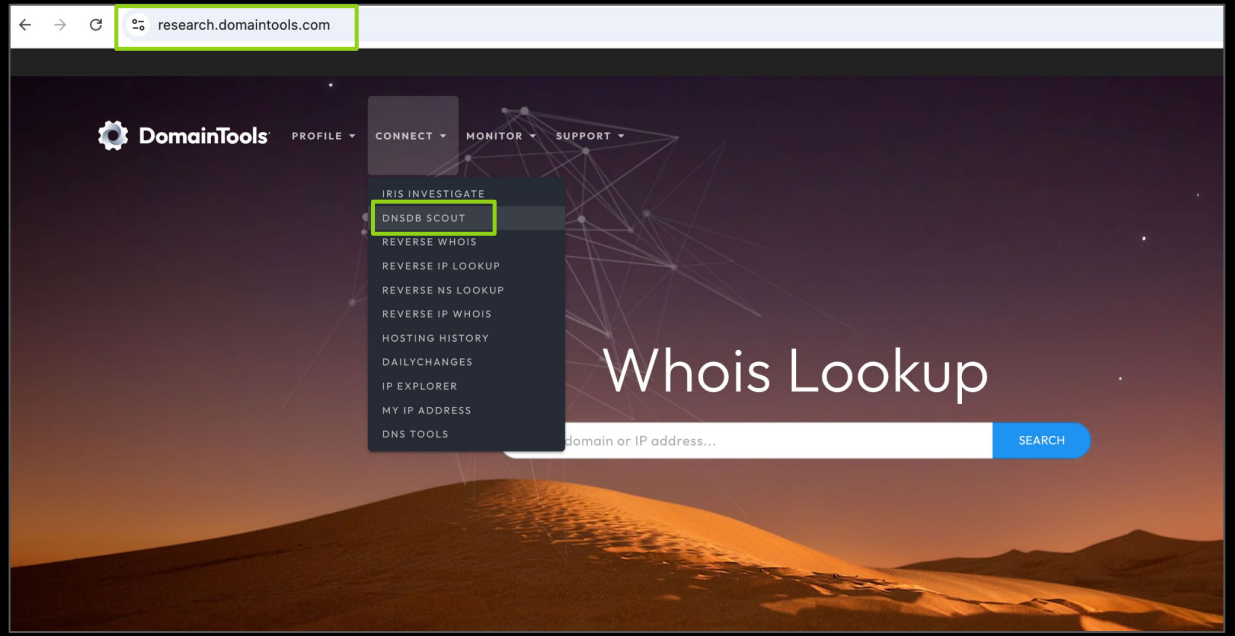
API owner receives email upon account creation.

02 Start Investigations

DNSDB can be started from the research home page.

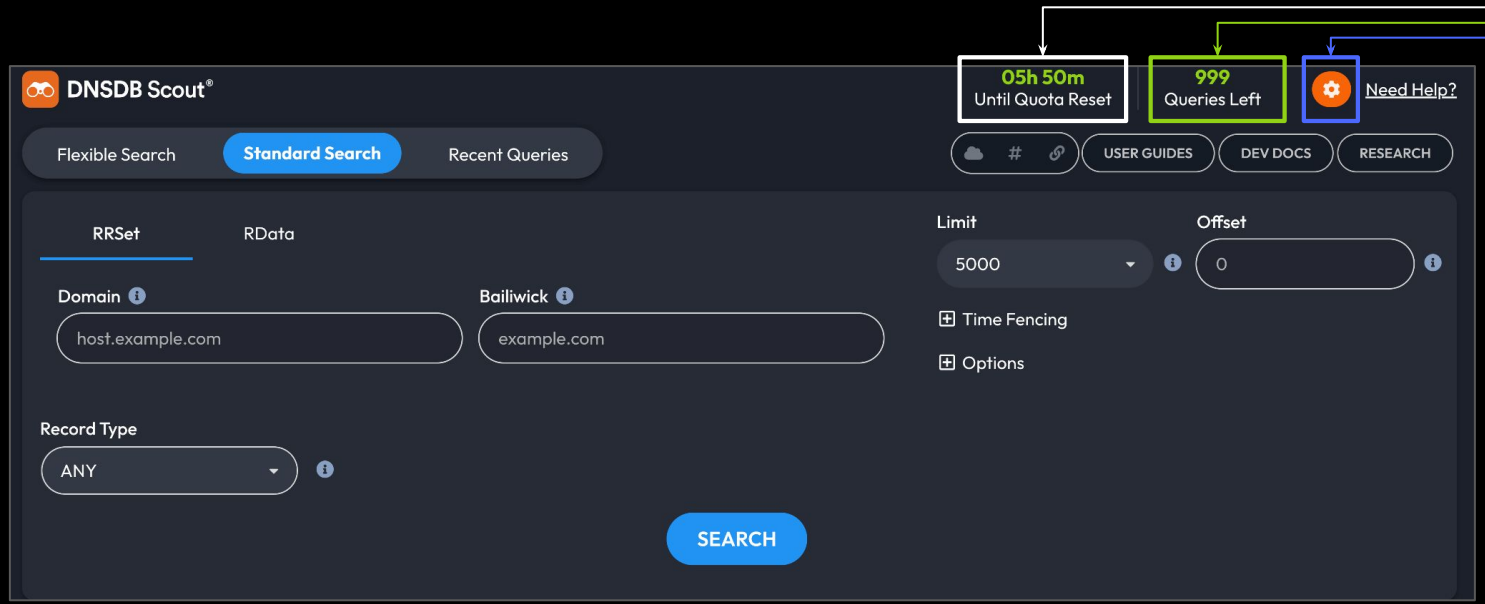
03 Direct Access

To access the platform directly, select ‘DNSDB Scout’ under the ‘Connect’ menu.



DomainTools

DNSDB Scout Home Page



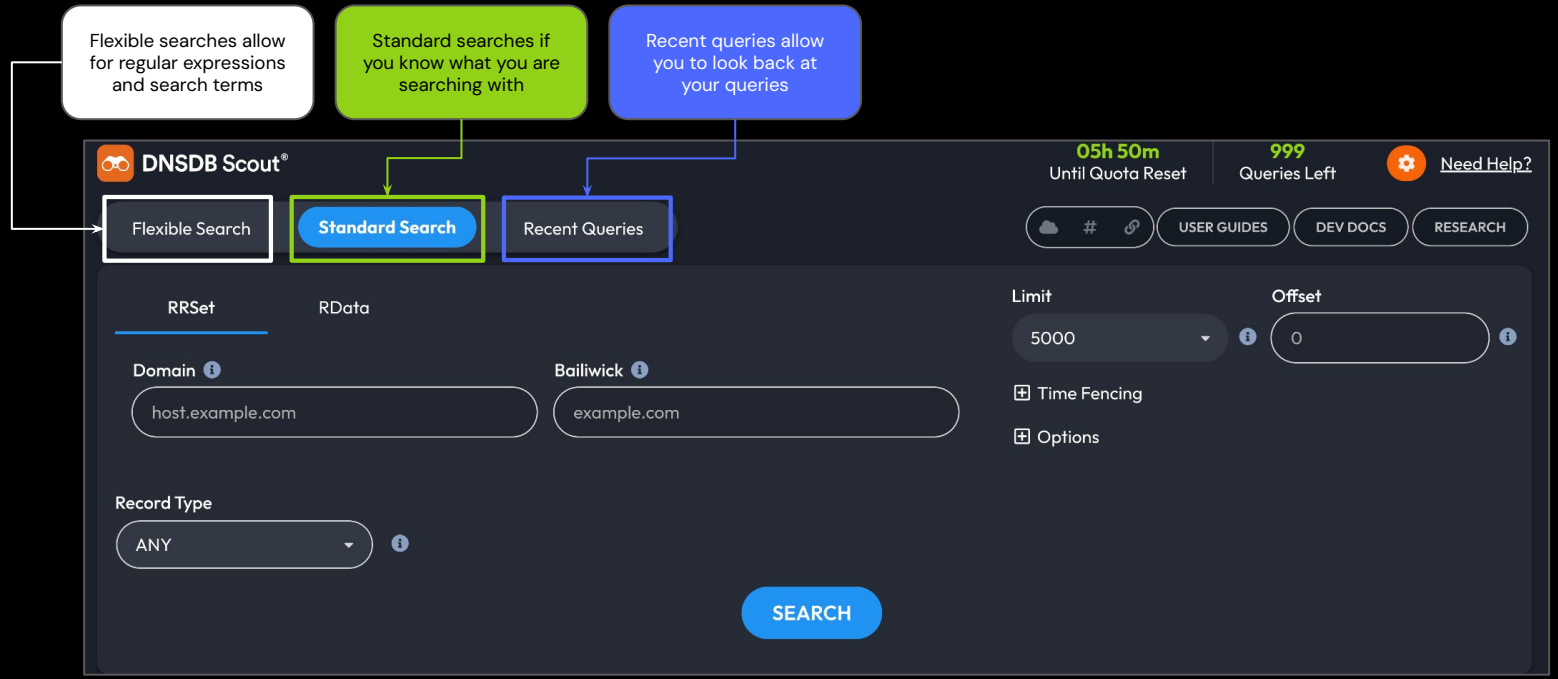
Time until DNSDB quota is reset

Total number of daily queries remaining

DNSDB Scout settings page

DomainTools

DNSDB Scout Home Page

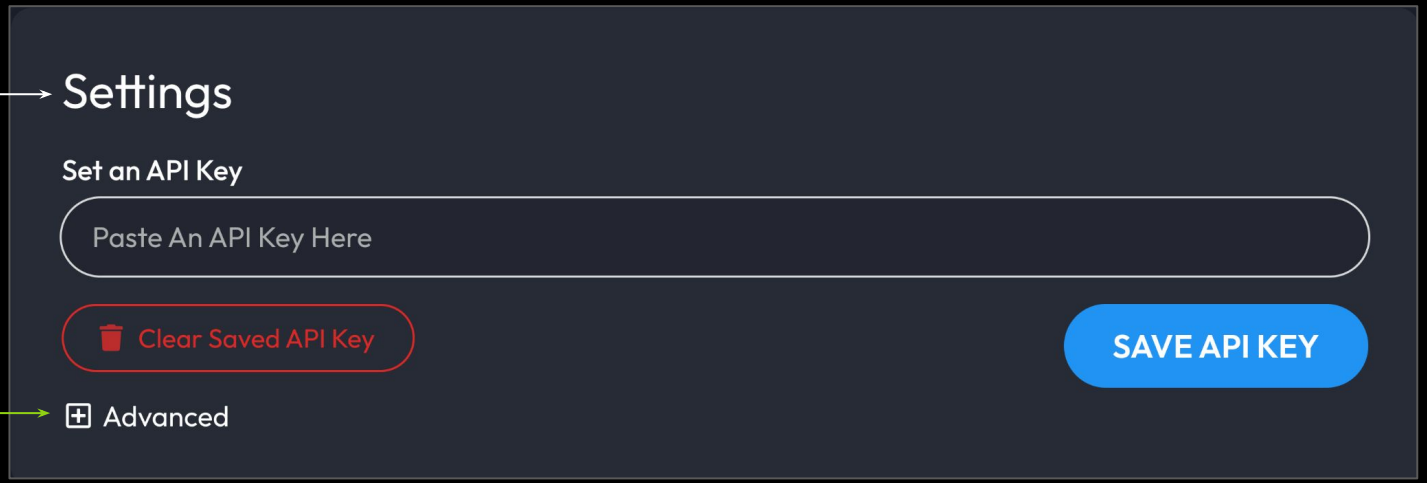


DomainTools

Getting Started

The Settings screen allows you to paste in your DNSDB API key for use with Scout

Advanced options allow the user to change further settings



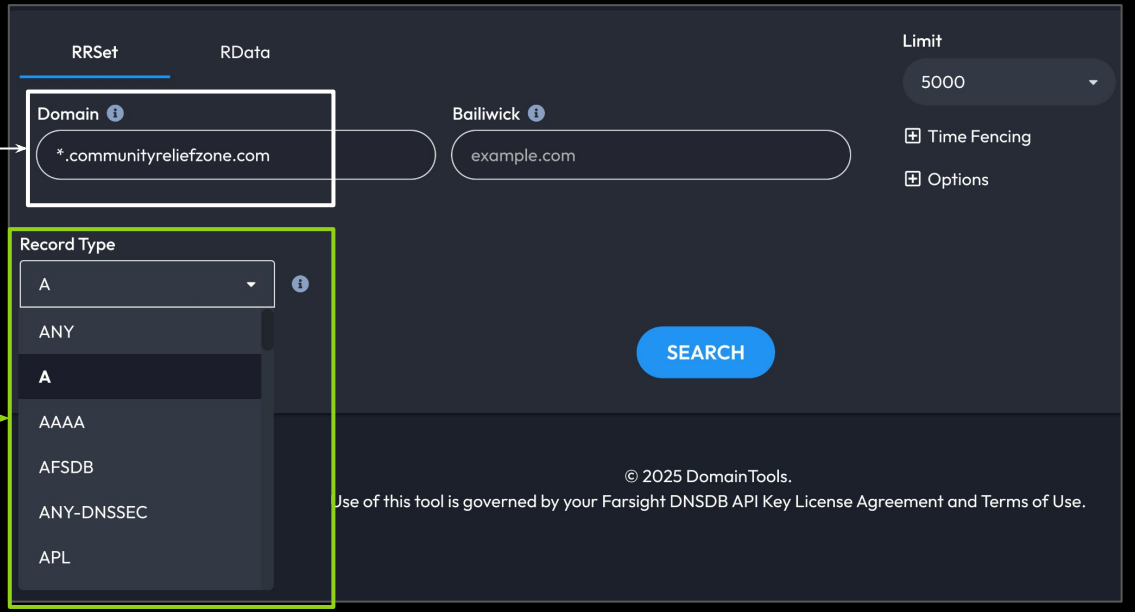
DomainTools

Getting Started

You can enter any type of domain in this box and DNSDB will provide the matches.

You can also utilize the left-side wildcard match (*.domain) or the right-side wildcard match (hostname.*)

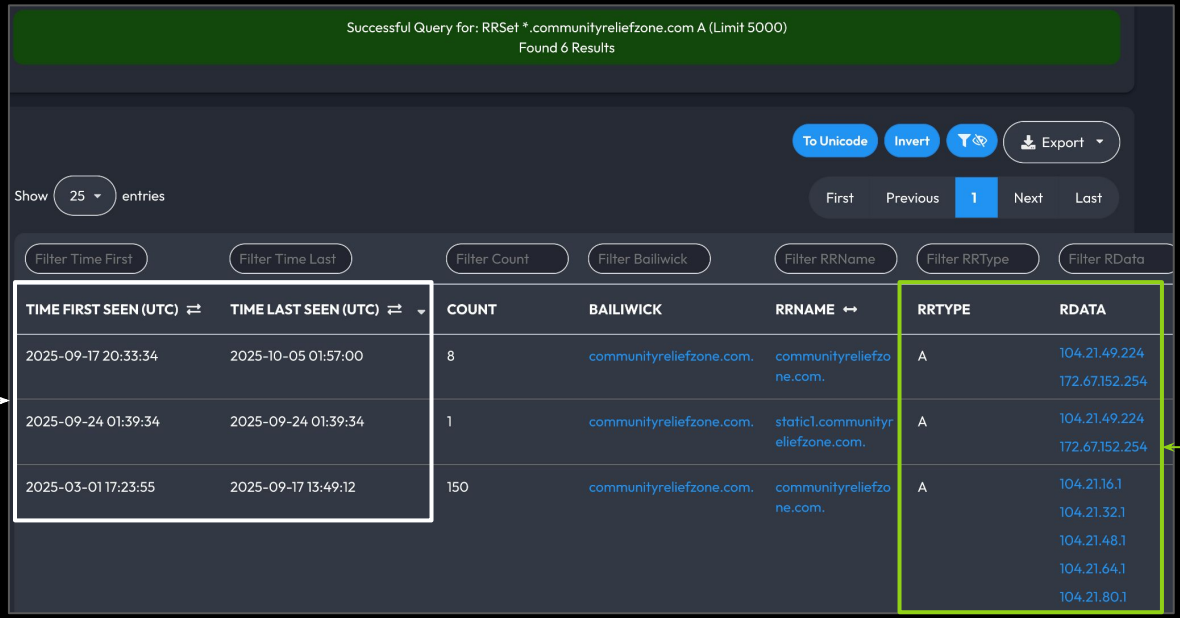
DNSDB can match against "ANY" resource record type, or you can choose a specific one.



DomainTools

Getting Started

Results will display both the Time First Seen and the Time Last Seen which provides the frame for the set of observations.



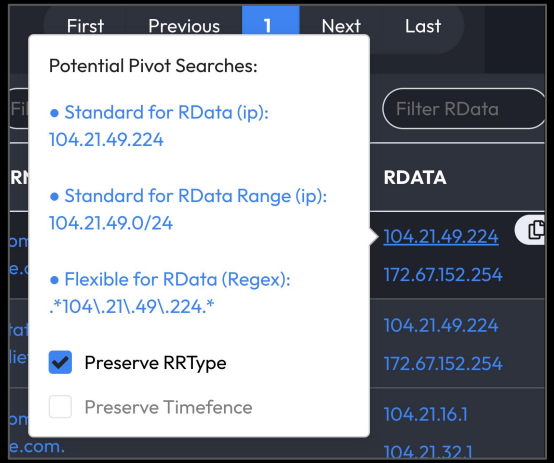
The resource record type (RRTYPE) and the response data (RDATA) are a unique observation set for any domain name that has been observed (RRNAME).

DomainTools

Getting Started

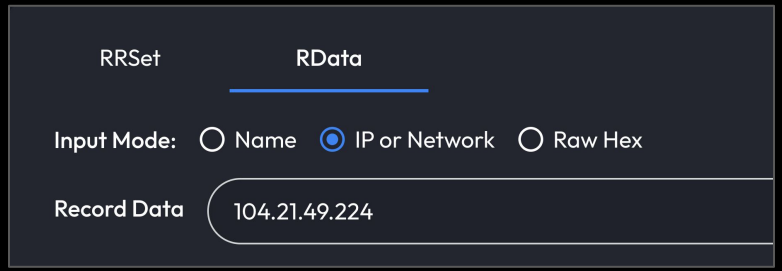
Pivoting

Hovering over the RDATA results gives you common options to pivot to additional queries.



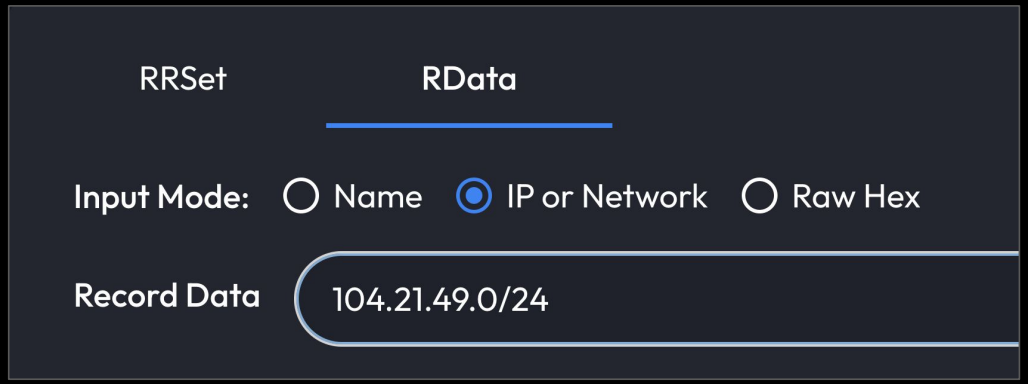
RDATA Pivoting

Clicking on a pivot pre-populates a new query with appropriate values.



DomainTools

Getting Started

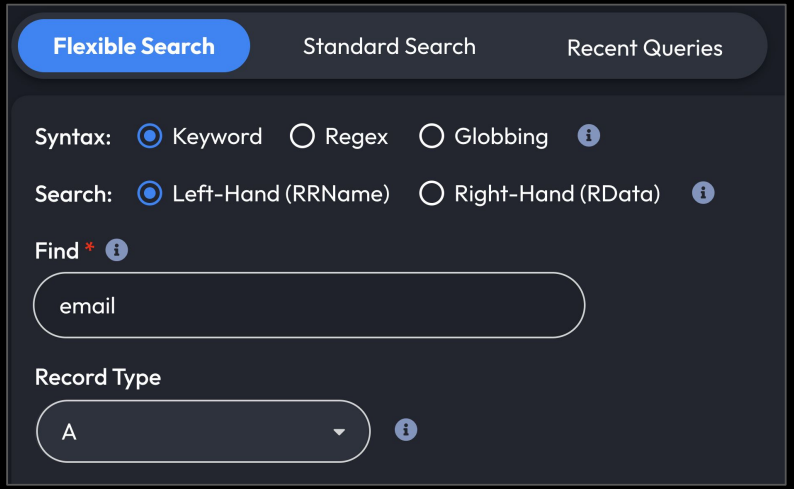


RDATA Search

You can also search by the RDATA or the response of a DNS query. Using an RDATA search allows you to search for a name (like a nameserver or mail server), IP address, or CIDR block. This example shows the CIDR notation.

DomainTools

Getting Started



Flexible Search

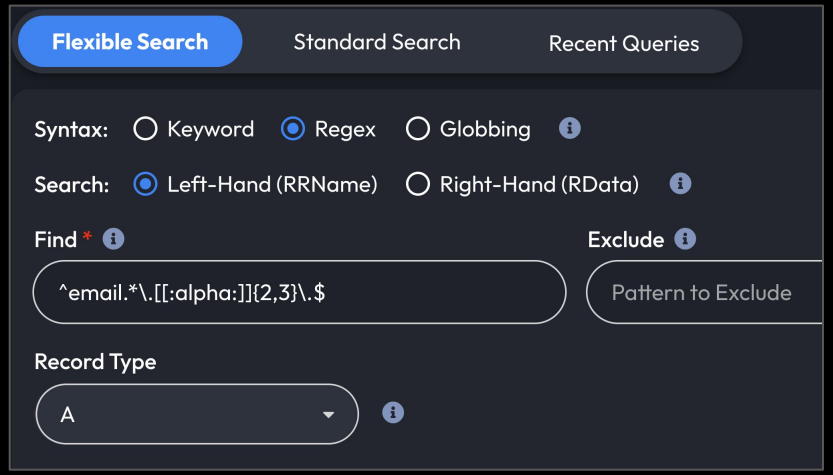
Using a Flexible Search allows you to use multiple syntax options. A Keyword search looks for the specific term that you requested.

Flexible Search Results

If that term exists somewhere in a domain name, it is considered a match and will be displayed in the results pane. Note that only the domain name and the resource record type are included in Flexible Search results.

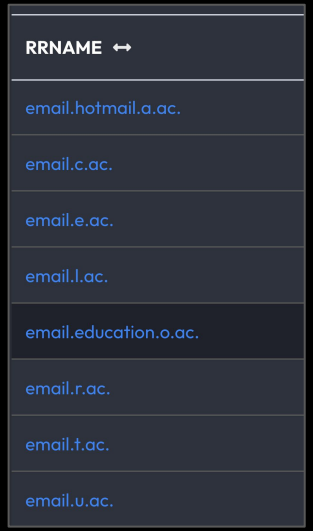
DomainTools

Getting Started



Regex Search

A Regex search allows you to use regular expressions. In this case, the domain must start with “email” and have a 2 or 3 letter TLD.

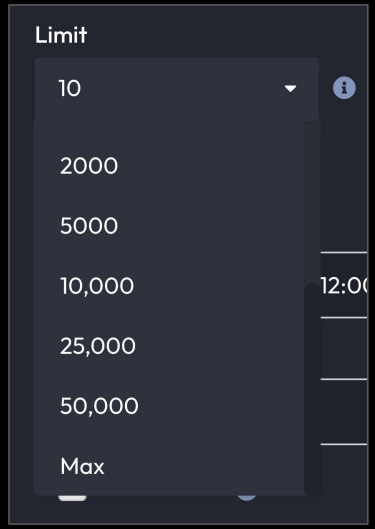


Regex Search Results

The results show domains that match this pattern.

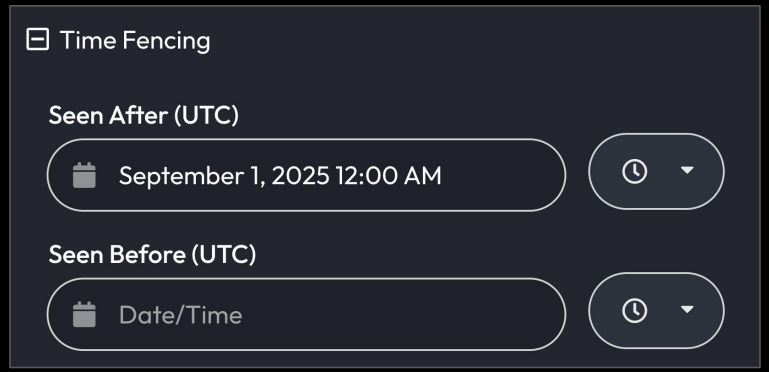
DomainTools

Additional Options



Response Limiting

The “Limit” allows you to put a limit on the number of responses you receive for your search. Anywhere from 10 results up to “Max” (which is 100,000).



Time Fencing

Time Fencing also allows you to specify a “Seen After” or “Seen Before” date and time. You can also use both options to set a specific time frame.

DomainTools


DomainTools