

DNSSDB 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



Getting Started

01 Account Activation

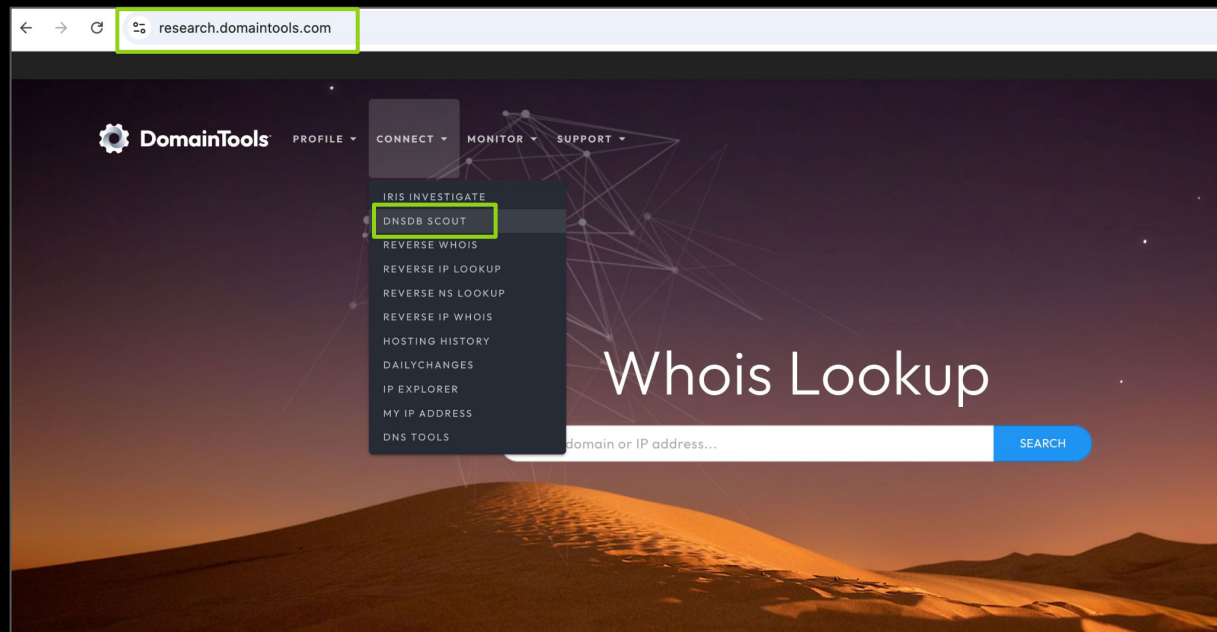
API owner receives email upon account creation.

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.



DNSDB Scout Home Page

The screenshot shows the DNSDB Scout Home Page. The interface includes a header with the DNSDB Scout logo, search tabs (Flexible Search, Standard Search, Recent Queries), and a top right section with status indicators and navigation links. The main search area has fields for Domain (host.example.com), Bailiwick (example.com), and Record Type (ANY), along with a SEARCH button. The right sidebar contains settings for Limit (5000) and Offset (0), and checkboxes for Time Fencing and Options. Annotations with colored boxes and arrows point to specific elements: a white box for '05h 50m Until Quota Reset', a green box for '999 Queries Left', a blue box for the settings gear icon, and a white box for 'Need Help?'. Arrows connect these boxes to callout boxes on the right: 'Time until DNSDB quota is reset' (white), 'Total number of daily queries remaining' (green), and 'DNSDB Scout settings page' (blue).

Annotations:

- Time until DNSDB quota is reset
- Total number of daily queries remaining
- DNSDB Scout settings page

DNSDB Scout Home Page

Flexible searches allow for regular expressions and search terms

Standard searches if you know what you are searching with

Recent queries allow you to look back at your queries

 **DNSDB Scout®**

Flexible Search

Standard Search

Recent Queries

05h 50m
Until Quota Reset

999
Queries Left

 [Need Help?](#)

[USER GUIDES](#)

[DEV DOCS](#)

[RESEARCH](#)

RRSet

RData

Domain ⓘ

Bailiwick ⓘ

host.example.com

example.com

Record Type

ANY ⓘ

SEARCH

Limit

5000 ⓘ

Offset

0 ⓘ

 Time Fencing

 Options

Getting Started

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

Settings

Set an API Key

Paste An API Key Here



Clear Saved API Key

SAVE API KEY

Advanced options allow the user to change further settings



Advanced



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.

The screenshot shows the DNSDB search interface. It has two tabs: 'RRSet' (selected) and 'RData'. In the 'RRSet' tab, there are two input fields: 'Domain' and 'Bailiwick'. The 'Domain' field contains '*.communityreliefzone.com' and is highlighted with a white border. The 'Bailiwick' field contains 'example.com'. To the right of these fields is a 'Limit' dropdown set to '5000'. Below the 'Domain' field is a 'Record Type' dropdown menu, which is open and shows a list of record types: A, ANY, A (highlighted), AAAA, AFSDb, ANY-DNSSEC, and APL. A blue 'SEARCH' button is located to the right of the 'Record Type' dropdown. At the bottom of the interface, there is a copyright notice: '© 2025 DomainTools. Use of this tool is governed by your Farsight DNSDB API Key License Agreement and Terms of Use.'

RRSet RData

Domain *i* *.communityreliefzone.com

Bailiwick *i* example.com

Limit 5000 *v*

+ Time Fencing

+ Options

Record Type

A *i*

ANY

A

AAAA

AFSDb

ANY-DNSSEC

APL

SEARCH

© 2025 DomainTools.
Use of this tool is governed by your Farsight DNSDB API Key License Agreement and Terms of Use.

Getting Started

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

Successful Query for: RRSet *.communityreliefzone.com A (Limit 5000)
Found 6 Results

To Unicode Invert Export

Show 25 entries

First Previous 1 Next Last

Filter Time First Filter Time Last Filter Count Filter Bailiwick Filter RRName Filter RRType Filter RData

TIME FIRST SEEN (UTC) ⇄	TIME LAST SEEN (UTC) ⇄	COUNT	BAILIWICK	RRNAME ⇄	RRTYPE	RDATA
2025-09-17 20:33:34	2025-10-05 01:57:00	8	communityreliefzone.com.	communityreliefzone.com.	A	104.21.49.224 172.67.152.254
2025-09-24 01:39:34	2025-09-24 01:39:34	1	communityreliefzone.com.	static1.communityreliefzone.com.	A	104.21.49.224 172.67.152.254
2025-03-01 17:23:55	2025-09-17 13:49:12	150	communityreliefzone.com.	communityreliefzone.com.	A	104.21.16.1 104.21.32.1 104.21.48.1 104.21.64.1 104.21.80.1

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

Getting Started

Pivoting

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

The screenshot shows a web interface with a table of RDATA results. A dropdown menu is open over the first row, displaying 'Potential Pivot Searches:' with three options: 'Standard for RData (ip): 104.21.49.224', 'Standard for RData Range (ip): 104.21.49.0/24', and 'Flexible for RData (Regex): *104\,21\,49\,224.*'. There are also checkboxes for 'Preserve RRTYPE' (checked) and 'Preserve Timefence' (unchecked). The table has columns for 'First', 'Previous', '1' (selected), 'Next', and 'Last'. The table content includes a 'Filter RData' button and a list of IP addresses: 104.21.49.224, 172.67.152.254, 104.21.49.224, 172.67.152.254, 104.21.16.1, and 104.21.32.1.

RDATA Pivoting

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

The screenshot shows a web interface with two tabs: 'RRSet' and 'RData' (selected). Below the tabs, there is an 'Input Mode' section with three radio buttons: 'Name', 'IP or Network' (selected), and 'Raw Hex'. Below this is a 'Record Data' section with a text input field containing '104.21.49.224'.

Getting Started

RRSet

RData

Input Mode: ☐ Name ☒ IP or Network ☐ Raw Hex

Record Data 104.21.49.0/24

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.



Getting Started

Flexible Search Standard Search Recent Queries

Syntax: ☒ Keyword ☐ Regex ☐ Globbing ⓘ

Search: ☒ Left-Hand (RRName) ☐ Right-Hand (RData) ⓘ

Find * ⓘ

email

Record Type

A ▼ ⓘ

Flexible Search

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

RRNAME ↔	RRTYPE
email.hotmail.a.ac.	A
email.c.ac.	A
email.e.ac.	A
securemail.e.ac.	A ⓘ
gsam-email-qa.e.ac.	A
gsam-email-prod.e.ac.	A
bucket-ns14bemail.e.ac.	A
application.bucket-ns14bemail.e.ac.	A
cgigistlientkb.application.bucket-ns14bemail.e.ac.	A
webgist.cgigistlientkb.application.bucket-ns14bemail.e.ac.	A

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.

Getting Started

Flexible Search

Standard Search

Recent Queries

Syntax:

☐ Keyword

☒ Regex

☐ Globbing

Search:

☒ Left-Hand (RRName)

☐ Right-Hand (RData)

Find

Exclude

Record Type

Regex Search

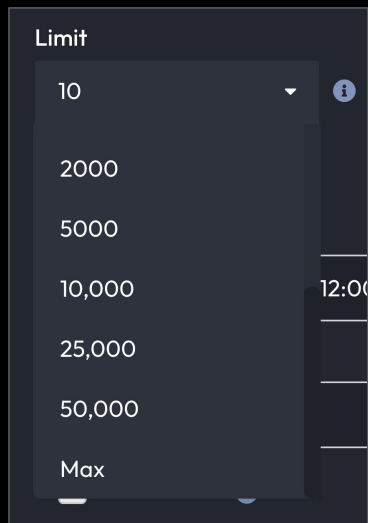
A Regex search allows you to use regular expressions. In this case, the domain must start with "email" and have a 2 or 3 letter TLD.

RRNAME ↔
email.hotmail.a.ac.
email.c.ac.
email.e.ac.
email.l.ac.
email.education.o.ac.
email.r.ac.
email.t.ac.
email.u.ac.

Regex Search Results

The results show domains that match this pattern.

Additional Options



A screenshot of a web interface showing a 'Limit' dropdown menu. The menu is open, displaying a list of options: 10, 2000, 5000, 10,000, 25,000, 50,000, and Max. The '10' option is currently selected. To the right of the dropdown, a portion of another dropdown menu is visible, showing '12:00'.

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

Seen After (UTC)



September 1, 2025 12:00 AM



Seen Before (UTC)



Date/Time



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