



# **DNSDB<sup>®</sup> Flexible Search**

## **An Introduction**

## About the Presenter



**Daniel Schwalbe**  
VP Engineering & Deputy CISO  
Farsight Security, Inc.



## What We'll Be Covering Today

- What is DNSDB<sup>®</sup> Flexible Search?
- What problem does Flexible Search solve?
- How to perform a “Keyword” search.
- A look at Regular Expressions.
- How to search SOA Rdata fields.
- A Rdata TXT search example.

- API documentation can be found at <https://docs.dnsdb.info>

# **Why Create DNSDB Flexible Search? What Problems Does it Solve?**

# **Standard Search in DNSDB API was (and is) a Great Product, BUT...**

- 1. Some seemingly simple searches were frustratingly difficult/impossible.**
  - *Example:* you couldn't just type in a brand (such as "rolex") and find all the domain names that included that string
- 2. You might get lots of results (but maybe *not* the precise ones you wanted).**
  - Standard DNSDB? LOTS of results/query (up to 1,000,000 results/query) & it supports additional "offset" queries, too (up to 3,000,000 more results)
  - Also lots of query qualifiers (limit by RRtype, timefencing, bailiwick, etc)
  - *BUT...* even when leveraging all available query qualifiers and asking for max results, a flood of results could still "crowd out" what you were after
- 3. Some right-hand side ("Rdata") was tricky to search in Standard DNSDB.**
  - For instance, historically you couldn't easily search TXT record Rdata for arbitrary strings, nor could you search SOA records for maintainer points of contact (or zone master DNS server names)

# DNSDB Flexible Search **FIXES ALL THESE ISSUES**

- Flexible Search knocks the chains off DNSDB API and puts it into overdrive. No other passive DNS product can keep up.
- DNSDB Flexible Search now allows you to:
  - Easily make simple keyword searches
  - Do precise "egrep-style" regular expression searches
  - Search selected "SOA" record fields plus other tricky-to-search Rdata searches (such as "TXT" record substring searches)
- Flexible Search is being bundled at **no additional charge** for all paid DNSDB API customers (and for all DNSDB API grant recipients).
  - Flexible Search is NOT included as part of DNSDB Free Community Edition
  - Flexible Search is also NOT (yet) available for DNSDB Export (aka "DNSDB On-premises")

# "Why are You Offering Such a Cool New Capability at No Charge?"

- **It's our way of giving back to you, our customers.** We've just had our 10<sup>th</sup> anniversary and Farsight is doing well. We appreciate having you as a customer, and this is our tangible way of showing a little of that "love."
- **Part of our company's mission is helping people "fight the good fights".** Flexible Search is going to be a powerful new analytic weapon.
- **We want to grow our market share.** We believe Flexible Search is a unique capability that will differentiate DNSDB and help to solidify our relationship with existing customers... and maybe attract some new users, too.
- **We'd like to increase per-customer DNSDB utilization.** DNSDB usage is tier-priced. We think existing customers will like Flexible Search and may end up using it and Standard DNSDB a lot, perhaps to the point where they decide its time to upgrade to a higher usage tier or even to DNSDB API Unlimited.

# "How Could I Use Flexible Search?"

## Some Obvious Usage Scenarios...

- **Anti-Phishing:** Find unexpected domains containing bank names or payment service names (many of those FQDNs may turn out to be phishing sites).
- **Brand Protection:** Discover domain names attempting to attract customers to knockoff merchandise sites that sell fake watches, fake athletic shoes, fake lifestyle medications, pirated software, etc.
- **Drug Enforcement:** Criminals sometimes illegally sell narcotics online without a prescription. LEOs can search DNSDB for domain names that include the names of controlled substances such as oxycodone, hydrocodone, etc.
- **Incident Handling:** Your syslogs can be a treasure trove if properly enriched.
- **Investigative journalism:** Now reporters can easily search domain names for the name of a candidate ('trump' or 'biden') or an issue ('covid' or 'riots').
- And this is just scratching the surface...



# We'll Largely be Using DNSDB Scout Website for Today's Examples

- DNSDB Scout® is best known as a browser extension for Chrome, Brave, and Firefox, but DNSDB Scout also exists as a standalone webpage accessible from popular browsers. (This eliminates the need for you to install a browser extension.)
- DNSDB Scout Web Edition can be accessed at <https://scout.dnsdb.info>
- From 10/20/2020 on, it will be running the new Flexible Search interface, as shown on the next slide.
- **Please note that free Community Edition DNSDB API keys CAN NOT be used to make Flexible Search queries. Free Community Edition keys WILL continue to work to make DNSDB Standard Searches.**

# The New DNSDB Scout Website (as of 10/20/2020)

The screenshot shows the DNSDB Scout search interface. At the top left is the logo and name 'DNSDB Scout'. At the top right, it says 'Unlimited Queries Left' and 'Need Help?'. Below the logo are three tabs: 'Flexible Search' (selected), 'Standard Search', and 'Recent Queries'. To the right of these tabs are two buttons: 'USER GUIDE' and 'DEV DOCS'. The main search area contains several controls: 'Syntax' with radio buttons for 'Keyword' (selected), 'Regex', and 'Globbing'; 'Search' with radio buttons for 'Left-Hand (RRName)' (selected) and 'Right-Hand (RData)'; 'Find \*' and 'Exclude' sections, each with an input field; 'Record Type' with a dropdown menu set to 'ANY'; 'Limit' with a dropdown menu set to '5000'; 'Offset' with an input field set to '0'; and a checkbox for 'Time Fencing (UTC)'. A large green 'SEARCH' button is at the bottom center. At the bottom of the page, there is a copyright notice and a disclaimer.

**DNSDB Scout** Unlimited Queries Left [Need Help?](#)

**Flexible Search** | Standard Search | Recent Queries [USER GUIDE](#) [DEV DOCS](#)

Syntax:  Keyword  Regex  Globbing [i](#)

Search:  Left-Hand (RRName)  Right-Hand (RData) [i](#)

Limit: 5000 [i](#) Offset: 0 [i](#)

Time Fencing (UTC)

Find \* [i](#) Exclude [i](#)

Keyword or Pattern to Find | Pattern to Exclude

Record Type: ANY [i](#)

**SEARCH**

© 2020 Farsight Security, Inc.  
Use of this tool is governed by your DNSDB API Key License Agreement and Farsight Security Terms of Use.

# Every Search Needs a Starting Point, a Loose Thread...

- This is usually NOT much of an obstacle for practicing cybersecurity SMEs:
  - Maybe you're investigating a **spamvertised site** you saw in an email or text
  - Or perhaps your starting point is a **malicious domain** you saw being used as a botnet command and control server, or as a malware dropping site.
  - With Flexible Search you don't even need a domain name *per se* anymore, just a word, a string, a brand name – **anything that people might use as part of a domain name**.
  - You can even just search for domains that match a pattern, such as the sometimes-crazy regex patterns that DGA researchers often reverse-engineer.
- Let's start with a simple brand protection example. You probably know that **Rolex**<sup>(TM)</sup> brand watches are heavily targeted by knockoff watch sellers. Can we use Flexible Search to find domain names that incorporate that string?

# A Simple “Keyword” Search Example

## RRname vs. Rdata: Which Should I be Searching?

- Fundamental to your DNSDB search is the decision of whether to search RRnames ("Left Hand Side") or Rdata ("Right Hand Side").
- To help you choose, consider a typical DNSDB "NS" resource record:

```
farsightsecurity.com. IN NS ns5.dnsmadeeasy.com.
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

RRname (left hand side)

Rdata (right hand side)

- A simple rule of thumb: **most initial search will be of RRnames** (e.g., left hand side data).
- Later, you'll be interested in making Rdata searches for things like finding all names that share a common name servers, but for now, most likely you'll be searching RRnames.



# Making A Keyword Search of RRnames for "rolex"

The screenshot shows the DNSDB Scout search interface. At the top left is the logo and name "DNSDB Scout". To the right, it says "Unlimited Queries Left" and "Need Help?". Below this are tabs for "Flexible Search", "Standard Search", and "Recent Queries", along with "USER GUIDE" and "DEV DOCS" buttons. The search configuration area includes: "Syntax" with radio buttons for "Keyword" (selected), "Regex", and "Globbing"; "Search" with radio buttons for "Left-Hand (RRName)" (selected) and "Right-Hand (RData)"; a "Find" input field containing "rolex"; an "Exclude" input field with the placeholder "Pattern to Exclude"; a "Record Type" dropdown menu set to "ANY"; a "Limit" dropdown menu set to "Max"; an "Offset" input field set to "0"; and a "Time Fencing (UTC)" checkbox. A large green "SEARCH" button is at the bottom center. Red boxes highlight the "Keyword" radio button, the "Left-Hand (RRName)" radio button, the "rolex" text, the "Record Type" dropdown, the "Limit" dropdown, and the "SEARCH" button. Red lines connect these boxes to each other, showing the flow of the search configuration.

# Some Results.

## To See FULL DETAILS For a Result, Click on It.

Show 10 entries

EXPORT AS CSV

EXPORT AS JSON

RRName ^	RRType
bestclonerolex.haohuanongcom.cn.	A
bestclonerolex.maigoocom.cn.	A
bestclonerolex.wo25b.cn.	A
bestclonerolex.wontime.cn.	A
bestclonerolex.yiqi800com.cn.	A
bestclonerolex.youboycom.cn.	A
bestclonerolex.yxfbn5.cn.	A
bestclonerolexwatches.6l5ksa.cn.	A
bestclonerolexwatches.6l5ksa.cn.	HINFO
bestclonerolexwatches.99114com.cn.	A

4,911 to 4,920 of  
62,286 Results

First Previous 1 ... 490 491 492 493 494 ... 6229 Next Last

# Clicking on A Result Sets Up A Standard DNSDB Search For That Name, Returning Full Details

Flexible Search **Standard Search** Recent Queries [USER GUIDE](#) [DEV DOCS](#)

**RRSet** RData

Domain **bestclonerolex.yxfb5.cn.** Bailiwick **example.com**

Record Type **ANY**

Limit **5000** Offset **0**

Time Fencing (UTC)

Options

**SEARCH**

Successful Query for: RRSet bestclonerolex.yxfb5.cn. ANY (Limit 5000)

Show **10** entries [EXPORT AS CSV](#) [EXPORT AS JSON](#)

Time Last Seen ↕	Time First Seen ↕	Count	Bailiwick	RRName ^	RRType	RData
2020-07-22 19:08:37	2020-07-22 19:08:37	2	yxfb5.cn.	bestclonerolex.yxfb5.cn.	A	107.151.162.115

# "I'm Finding Too Many Hits, Or Hits For Really Old Domains That Are Of No Interest To Me!"

- DNSDB includes results that go back over a decade now.
- If you only care about "recent" results, use time fencing to restrict your query to names that have last been seen in the last year, last quarter, last month, last week, etc.
- Let's try doing that for our Rolex query...
- We'll just ask for domains that have been seen since September 21st, 2020.

# Time Fencing Our Previous Rolex Query



Unlimited  
Queries Left



[Need Help?](#)

Flexible Search

Standard Search

Recent Queries

[USER GUIDE](#)

[DEV DOCS](#)

Syntax:  Keyword  Regex  Globbing ?

Search:  Left-Hand (RRName)  Right-Hand (RData) ?

Find \* ?

rolex

Exclude ?

Pattern to Exclude

Record Type

ANY ?

Limit

Max ?

Offset

0 ?

Time Fencing (UTC)

Last Seen Before  Last Seen After

First Seen Before  First Seen After

?

SEARCH

Successful Query for: Glob RRNames rolex ANY (Limit 50000) // Last After: 2020-09-21 00:00:00 (UTC)  
Found 35759 Results



# A Few of the Time Fenced Results From That Query

Show 10 entries

EXPORT AS CSV

EXPORT AS JSON

RRName	RRType ^
bestrepicarolexwatchesuk.datasuns.com.cn.	A
dirtcheapfakerolexwatches.datasuns.com.cn.	A
bestrolexsubmarinerreplica.datasuns.com.cn.	A
repicarolexwatchesforsale.datasuns.com.cn.	A
ukswissrolexreplicawatches.datasuns.com.cn.	A
bestqualityswissrepicarolex.datasuns.com.cn.	A
rolexseadwellerdbluepricerreplica.datasuns.com.cn.	A
prolexis.com.cn.	A
www.prolexis.com.cn.	A
repicarolexsale.chongyatu.com.cn.	A

361 to 370 of 35,759  
Results

First Previous 1 ... 35 36 37 38 39 ... 3576 Next Last

## Some Tips

- Need help in the Scout interface? Try hovering over the **little purple circle "i" (information) icons**.
- After you've done multiple searches, you may try to use your browser's back arrow to go back to an earlier search. That won't work. Use Scout's **"Recent Queries" tab** to get at prior queries ("View" will show your cached results; "Re-Run" will re-run that query).
- The double chevrons at the end of each row of recent queries reveal the request URL that generated the query, as well as additional headers and the response that the API server returned as a result of the query. This is a useful tool to learn how to make your own queries against the DNSDB API.
- While simple string searches in DNSDB Scout's Flexible Search are called **"Keyword"** searches, you can also look for arbitrary alphanumeric characters -- **the search string does not need to be a "real English word."**
- While we used the keyword setting, **we could also just have easily used the regex search box** – it will also do the "right thing" if you just plug in an alphanumeric string.

## "Q. Back up a Minute -- Couldn't I Always Search DNSDB for a String that was Part of a Name?"

- No. Standard DNSDB API allowed (and still allows) you to search for:
  - **exact** domain name matches (such as **www.microsoft.com** )
  - **whole-label** left hand side wildcards (such as **\*.microsoft.com** ), and
  - **whole-label** right hand side wildcards (such as **www.microsoft.\*** )
- If you tried searching for an arbitrary string/**partial label** (such as **"icrosof"** ) in Standard DNSDB API, that would NOT match anything

DNSDB Flexible Search makes it trivial to find domains matching **any arbitrary string** of your choice, including a partial label such as **"icrosof"**

## "Q. Are Any (or All!) of Those Names We Discovered 'Bad' Ones?"

- Farsight objectively reports factual DNS data. We DON'T attempt to subjectively evaluate domain names and "rate" them as "good" or "bad" – different people may view the same name completely differently.
- Some names may certainly LOOK "**suspicious**" BUT a "suspicious-looking name" is just a **LEAD to check**, it ISN'T **actual PROOF of badness**.
- Some names mentioning a brand may actually belong to the brand owner.
- Some previously-seen domains may no longer be registered nor resolve.
- Yet other names may be "parked" and just trying to attract "eyeballs" for ads.
- Other names may be totally unrelated to a given brand and just coincidentally include the brand name as part of some longer word.
- **Therefore, carefully assess anything you come across BEFORE taking action!**
- One option? **Use a 3<sup>rd</sup>-party domain name reputation service provider.**

## "Q. I Think Some Stuff is 'Missing' in My Flexible Search Output!"

- **Important Concept:** DNSDB Flexible Search is **NOT** meant to be a "replacement" for DNSDB Standard Search.
- Flexible Search is a **FINDING AID** that **enhances** Standard Search.
- Flexible Search RRname searches intentionally do not return Rdata. Flexible Search Rdata searches intentionally do not return RRnames.  
**For full details, chase Flexible Search results in DNSDB Standard Search.**
- You will also **STILL need to use Standard Search to do certain types of routine queries.** For example, Flexible Search can't be used to search for IP addresses (or IP address ranges, or CIDR netblocks). Those queries are all ones that still get made via Standard Search.
- The real power of Flexible Search shows up when you begin to use **regular expressions.**



# Regular Expressions

# Why Bother with Regular Expressions?

- Some searches in Standard DNSDB API (even when written to take maximal advantage of all available query limitation options) may still yield an overwhelming number of results -- sometimes to the point of "crowding out" results you actually care about. **Flexible Search helps overcome this issue.**
- **Regular expressions are the "gold standard" for pattern matching.** Many users may already be familiar with regexes, but even if you've never touched a regular expression, you'll quickly pick up how they work.
- Distilled to its most basic, a **"regular expression" is just a pattern.** If the searched record matches the defined pattern, it gets returned as a hit.
- *Important Detail:* There are several different "flavors" or "styles" of regex. **DNSDB Flexible Search uses a flavor of "regular expression" known as "extended regular expressions," as used by the Un\*x *egrep* command.**
- Let's look at some *egrep-style* regular expression basics.

# A Small egrep-style Regular Expression "Cheat Sheet by Example"

- `.` dot means match any one character
- `\.` backslash dot means match a literal ("real") dot
- `.*` dot star matches any zero or more characters
- `north.*bank` match the string `north`, followed by anything (or nothing), followed by the string `bank`
- `(red|black|white)` match the string `red` or `black` or `white`
- `^www` the caret means this pattern must begin with `www`
- `\.com\.$` the dollarsign means this pattern must end with `.com.`
- `dark.{0,5}night` match the literal string `dark`, followed by any 0-5 characters, followed by the literal string `night`
- `^ns[c-e3-7]` the pattern must begin with `ns` followed by any one of the letters `c`, `d`, or `e`, or any one of the digits `3`, `4`, `5`, `6`, or `7`

This just scratches the surface, there's a **LOT** more you can do with regular expressions.

## "I Want Something Comprehensive on Regexes..."

- Farsight Blog Article: **"What's a Regular Expression?"**  
<https://www.farsightsecurity.com/blog/txt-record/regexp-20200804/>
- O'Reilly Book: **Introducing Regular Expressions**,  
[https://www.amazon.com/\\_/dp/1449392687](https://www.amazon.com/_/dp/1449392687)
- O'Reilly Book: **Mastering Regular Expressions**,  
[https://www.amazon.com/\\_/dp/0596528124](https://www.amazon.com/_/dp/0596528124)
- O'Reilly Book: **Regular Expressions Cookbook**,  
[https://www.amazon.com/\\_/dp/1449319432](https://www.amazon.com/_/dp/1449319432)
- O'Reilly Book: **Regular Expression Pocket Reference**,  
[https://www.amazon.com/\\_/dp/0596514271](https://www.amazon.com/_/dp/0596514271)

# An Example: Find Names that Mention covid or corona and Which End in Either .com. or .net.

The screenshot shows the DNSDB Scout search interface. The 'Flexible Search' tab is active. The 'Syntax' section has 'Regex' selected. The 'Search' section has 'Left-Hand (RRName)' selected. The 'Find' input field contains the regex `(corona|covid).*\.(com|net)\.$`. The 'Record Type' dropdown is set to 'ANY'. A 'SEARCH' button is visible. A green dashed arrow points from a callout box to the 'Find' input field. The callout box contains the text: 'Decoding that regular expression: (corona|covid) match either literal string .\* match anything or nothing \.(com|net)\.\$ pattern must END WITH either .com. or .net.'. At the bottom, a green box displays the search results: 'Successful Query for: Regex RRNames (corona|covid).\*\.(com|net)\.\$ ANY (Limit 50000) Found 50656 Results'.

Unlimited Queries Left

Need Help?

USER GUIDE DEV DOCS

Flexible Search Standard Search Recent Queries

Syntax:  Keyword  **Regex**  Globbing

Search:  Left-Hand (RRName)  Right-Hand (RData)

Limit: Max Offset: 0

Time Fencing (UTC)

Find \* `(corona|covid).*\.(com|net)\.$`

Exclude: Pattern to Exclude

Record Type: ANY

**SEARCH**

Successful Query for: Regex RRNames (corona|covid).\*\.(com|net)\.\$ ANY (Limit 50000) Found 50656 Results

**Decoding that regular expression:**  
-----  
`(corona|covid)` match either literal string  
`.*` match anything or nothing  
`\.(com|net)\.$` pattern must END WITH either .com. or .net.



# Sample Results

Show  entries

EXPORT AS CSV

EXPORT AS JSON

RRName	RRType
coronavirus.br.com.	NS
coronavirus.br.com.	SOA
corona.allianzinvestors.br.com.	A
anticoronahandgel.br.com.	CNAME
coronala.bs.com.	A
desktop-covidemo.ccng.bt.com.	TXT
desktop-covidevops.ccng.bt.com.	TXT
coronado.bw.bw.com.	A
corona-po.bw.bw.com.	A
corona-pad3.bw.bw.com.	A

661 to 670 of 50,656 Results

First

Previous

1

...

65

66

67

68

69

...

5066

Next

Last

# Debugging Some Potential Regex Issues

- If you see *"Error: Keywords are restricted to non-Unicode alphanumerics, dashes, underscores, and dots. Try the Regex syntax for more options."* that means you didn't remember to hit Scout's "Regex" search button. Click the "Regex" button & try it again.
- All regex patterns should include at least two contiguous non-wildcard characters (a non-wildcard character followed by a dot and a 2<sup>nd</sup> non-wildcard character is also OK).
- If searching Rdata for IP addresses, IP address ranges, or CIDR netblocks, those queries should be made in DNSDB Standard Search. Why? **Only CNAME, HINFO, MX, NAPTR, NS, PTR, RP, SOA, SPF, SRV, TXT get their Rdata indexed** ("A" and "AAAA" records do NOT).
- SOA records get truncated to just **mname**, space, **rname** for indexing.
- DNSSEC records don't get indexed in Flexible Search, nor do records where EITHER the RRname is >81 characters long OR the Rdata is >256 characters long.
- The most common regular expression "issue" area? **Right anchored regular expression search patterns**. Perhaps you just want to get hits from the dot edu TLD. **If so, remember that ALL Flexible Search RRnames end with a formal dot**. Thus to match names ending dot edu, you'd specify:  
`\.edu\.$`

# A Cool New DNSDB Flexible Search Feature: **EXCLUSIONS**

- Another new and unique capability of DNSDB Flexible Search is the ability to exclude known-**UN**wanted names.
- For example, pandemic-related names would likely NOT include:

**coronado** *or*

**coronation** *or*

**covideo** *or*

**covidien**

...BUT those names would normally be found and returned if we asked to match names that have the substring **corona** or **covid**.

- By using a Flexible Search exclusion pattern, we can rerun our search and exclude names containing any of those strings.

# Re-Running Our Search with an Exclusion Rule

The screenshot shows the DNSDB Scout search interface. At the top, there's a navigation bar with the DNSDB Scout logo, 'Unlimited Queries Left', and a 'Need Help?' link. Below this are tabs for 'Flexible Search', 'Standard Search', and 'Recent Queries', along with 'USER GUIDE' and 'DEV DOCS' buttons. The search configuration area includes options for 'Syntax' (Keyword, Regex, Globbing) and 'Search' (Left-Hand (RRName), Right-Hand (RData)). The 'Find' field contains the regex '(corona|covid).\*\.(com|net)\. \$' and the 'Exclude' field contains '(coronado|coronation|covid|covi'. The 'Record Type' is set to 'ANY'. A 'SEARCH' button is prominently displayed. Below the search area, a green box contains the query details: 'Successful Query for: Regex RRNames (corona|covid).\*\.(com|net)\. \$ ANY (Limit 50000) [Excl. (coronado|coronation|covid|covidien)] Found 50599 Results'.

Unlimited Queries Left

Need Help?

Flexible Search Standard Search Recent Queries

USER GUIDE DEV DOCS

Syntax:  Keyword  Regex  Globbing

Search:  Left-Hand (RRName)  Right-Hand (RData)

Limit: Max Offset: 0

Time Fencing (UTC)

Find: (corona|covid).\*\.(com|net)\. \$

Exclude: (coronado|coronation|covid|covi

Record Type: ANY

SEARCH

Successful Query for: Regex RRNames (corona|covid).\*\.(com|net)\. \$ ANY (Limit 50000) [Excl. (coronado|coronation|covid|covidien)] Found 50599 Results

# Some Results

Show 10 entries

EXPORT AS CSV

EXPORT AS JSON

RRName	RRType
corona.chaletcert-1.8x8.com.	A
global-corona.chaletcert-1.8x8.com.	A
corona.chaletcert-2.8x8.com.	A
global-corona.chaletcert-2.8x8.com.	A
corona.chaletchalet.8x8.com.	A
global-corona.chaletchalet.8x8.com.	A
corona.chaletcicril.8x8.com.	A
global-corona.chaletcicril.8x8.com.	A
corona.chaletclient.8x8.com.	A
global-corona.chaletclient.8x8.com.	A

49,631 to 49,640 of 50,599 Results

First

Previous

1

...

4962

4963

4964

4965

4966

...

5060

Next

Last

## Some Quick Notes About Exclusions

- Our sample exclusion pattern consisted of four string literals, but you can *exclude* any regex that you could have entered as a pattern to *match*. (If you're accustomed to working with the Un\*x **egrep** command, think of a Flexible Search exclusion as being kin to how **egrep --invert-match** works).
- Exclusions are made based **ONLY** on what's in RRnames (if you're searching RRnames), or **ONLY** on what's in Rdata (if you're searching Rdata).
- If you run a search without an exclusion expression & then rerun it **with** an exclusion expression, that counts as **TWO** queries (e.g., the rerun-with-exclusion is a brand new search, NOT just a tweaking of results that have already been received and cached).
- **Important: there may be MORE THAN the 50,000 unique hits that DNSDB Scout knows about, even WITH exclusions. You can use the "Offset" feature to "jump ahead" by a specific number of results (perhaps 50,000, to get past the ones you've already seen), so that you can see more results...**

# Rerunning Our Search With A 50,000 Result Offset



DNSDB Scout®

Unlimited  
Queries Left

IDN/Punycode Status  
✓ Supported



[Need Help?](#)

Flexible Search

Standard Search

Recent Queries

[USER GUIDE](#)

[DEV DOCS](#)

Syntax:  Keyword  Regex  Globbing ?

Search:  Left-Hand (RRName)  Right-Hand (RData) ?

Find \* ?

(corona|covid)\*\.(com|net)\.\$

Exclude ?

(coronado|coronation|coveideo|covidien)

Record Type

ANY ?

Limit

Max ?

Offset

50000 ?

Time Fencing (UTC)

SEARCH

Successful Query for: Regex RRNames (corona|covid)\*\.(com|net)\.\$ ANY (Limit 50000) [Excl. (coronado|coronation|coveideo|covidien)] (Offset 50000)  
Found 50000 Results



# Some Results

Show  entries

EXPORT AS CSV

EXPORT AS JSON

RRName	RRType ^
corona.chalet.maskurmuslim.8x8.com.	A
global-corona.chalet.maskurmuslim.8x8.com.	A
cocovida.maskurmuslim.8x8.com.	A
coronaliu.maskurmuslim.8x8.com.	A
global-corona.maskurmuslim.8x8.com.	A
mcp-cocovida.8x8.com.	A
mcpcoronaliu.8x8.com.	A
mdm-cocovida.8x8.com.	A
mdmcoronaliu.8x8.com.	A
meetcocovida.8x8.com.	A

141 to 150 of 50,000 Results

First Previous 1 ... 13 14 15 16 17 ... 5000 Next Last

[↻ Re-Run Query With Max Limit Offset](#)



## Some Quick Notes About Offsets

- DNSDB's data is continually being updated. If you were to do three 50,000 queries in Scout in close succession, all for the same query (but with offsets of 0, 50,000 and 100,000) you might end up with less than 150,000 unique names as a result (e.g., we do NOT "freeze" a gazillion results and then just page through those cached results for subsequent offset requests).
- EACH offset query you make is a NEW query. This means that if you do a query with an offset of 0, a query with an offset of 50,000 and a query with an offset of 100,000, you've used up three queries (remember, you're not just moving forward through the "saved results" from some single "mega query").
- The largest allowed offset in Scout is 3,000,000. This means your "visibility horizon" in Scout is 3,050,000 (3,000,000 offset + Scout's 50,000 max results).

# "We've Been Talking About Regexes. What About Globbing?"

- We suspect that most people won't even know what globbing is. (If you *have* run into globbing before, it was probably in conjunction with selecting file names at the command prompt in a terminal window.)
- **Most users should probably just stick to regex searches**
- If you **really** want to try our globbing implementation as an alternative, it follows the Un\*x glob(7) syntax, see <https://man.openbsd.org/glob.7>
- A brief overview of Globbing is available in the blog article "What's Globbing?" See <https://www.farsightsecurity.com/blog/txt-record/glob-20200804/>
- **Our most important globbing tip is this:** remember to surround your glob pattern with asterisks (or at least end your pattern with a dot) since every glob search is implicitly anchored on the left and the right, and every RRname ends with a formal dot.

# Searching Select SOA Rdata Fields

# We Searched RRnames, but We Can ALSO Search Rdata

- Our sample "rolex" search was made on RRnames ("Left Hand Side") data.
- Sometimes we may also want to search in Rdata ("Right Hand Side") data.
- DNSDB Flexible Search can search EITHER side, just click on the appropriate button in the DNSDB Scout interface.
- Searching Rdata can be trickier than RRnames because Rdata can take many different forms, including domain names, IPv4 and IPv6 addresses, text data, and even complex records containing multiple fields (such as SOA records).
- Standard DNSDB Search works just fine for IP addresses, IP ranges, and CIDR netblocks (plus exact domain names and whole label domain name wildcards).
- Historically, however, it's been hard to make arbitrary Rdata string searches, or to search SOA Rdata using DNSDB Standard Search.
- That's all been addressed in Flexible Search.

# Flexible Search Really Opens up Rdata Searches

- You've seen Flexible Search for **RRnames**.
- Flexible Search also indexes **Rdata** for an enumerated set of RRtypes: CNAME, HINFO, MX, NAPTR, NS, PTR, RP, SOA, SPF, SRV, and TXT RRtypes.
- Searching Rdata in Flexible Search is normally a **multistep process**:
  - **The 1st step** may be a matter of figuring out what you want to find in Rdata either in DNSDB Standard Search or elsewhere.
  - **The 2nd step** will normally be a DNSDB Flexible Search that matches a specified string. Each hit will be associated with a Flexible Search raw hex query string.
  - **The 3rd step** will be one or more Standard DNSDB Searches, done with the magic raw hex query string or strings you found in step 2. The 3<sup>rd</sup> step search (or searches) will yield the results we actually want. Let's look at an example.

# Uncovering Hidden Connections in DNS SOA Data

- Assume we're interested in identifying all domains related to **bloomborg.com**
- While there might be many ways to identify domains related to **bloomborg.com**, let's try try using **zone point of contact (POC) addresses**, as shown in the domains Start of Authority (SOA) record.
- Historically it has been quite tricky to search that data in Standard DNSDB. Fortunately, DNSDB Flexible Search now indexes the SOA point of contact and master server name (but NOT other SOA fields such as serial numbers and time-to-live (TTL) values).
- The first thing we need is the point of contact address for a known bloomborg.com domain (such as bloomborg.com itself). We'll look that up in DNSDB Standard Search. This is "step one" of the three step process.
- See the next slide.



# DNSDB Standard Search for bloomberg.com SOA

The screenshot shows the DNSDB Scout interface. At the top left is the logo and name "DNSDB Scout®". On the top right, it says "Unlimited Queries Left" and "Need Help?". Below the header are three tabs: "Flexible Search", "Standard Search" (highlighted with a red box), and "Recent Queries". To the right of these tabs are two buttons: "USER GUIDE" and "DEV DOCS".

Below the tabs are two sub-tabs: "RRSet" (highlighted with a red box) and "RData". Under "RRSet", there are two input fields: "Domain" containing "bloomberg.com" (highlighted with a red box) and "Bailiwick" containing "example.com". Below these is a "Record Type" dropdown menu set to "SOA" (highlighted with a red box). To the right of the search fields are controls for "Limit" (set to 5000) and "Offset" (set to 0). There are also expandable sections for "Time Fencing (UTC)" and "Options". A green "SEARCH" button (highlighted with a red box) is located at the bottom right of the search area.

At the bottom of the interface, a green banner displays the message: "Successful Query for: RRSet bloomberg.com SOA (Limit 5000) Found 940 Results".

# bloomberg.com SOA Results

Time First Seen ↕	Time Last Seen ↕ ▾	Count	Bailiwick	RRName	RRType	RData
2020-09-25 20:19:34	2020-09-27 00:28:20	33762	bloomberg.com.	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307376 9 43200 3600 3600000 14400
2020-09-24 20:01:22	2020-09-26 05:46:03	48753	bloomberg.com.	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307376 8 43200 3600 3600000 14400
2020-09-22 01:42:16	2020-09-24 20:01:54	267492	bloomberg.com.	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307376 7 43200 3600 3600000 14400
2020-09-19 06:07:07	2020-09-22 11:23:27	116479	bloomberg.com.	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307376 6 43200 3600 3600000 14400
2020-09-17 20:26:05	2020-09-19 07:21:33	58155	bloomberg.com.	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307376 5 43200 3600 3600000 14400

# DNSDB Flexible Search for dnsmaster.bloomberg.com in SOA Rdata

The screenshot shows the DNSDB Scout interface with the following configuration:

- Search Mode:** Flexible Search (highlighted with a red box).
- Syntax:** Regex (selected with a red box).
- Search Target:** Right-Hand (RData) (selected with a red box).
- Find:** dnsmaster\.bloomberg\.com\.\$ (highlighted with a red box).
- Record Type:** SOA (highlighted with a red box).
- Limit:** Max.
- Offset:** 0.
- Time Fencing:** UTC (checked).


A green **SEARCH** button is visible below the configuration fields.

A green notification bar at the bottom of the interface displays the following message: **Successful Query for: Regex RData dnsmaster\.bloomberg\.com\.\$ SOA (Limit 50000)** (highlighted with a red box).

# Initial Results from our Flexible Search SOA Rdata Query

Show  entries

[EXPORT AS CSV](#) [EXPORT AS JSON](#)

RRTYPE	RData	
SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com.	<b>This ==&gt;</b> 

1 to 1 of 1 Results

[First](#) [Previous](#) **1** [Next](#) [Last](#)

- Notice the magic link icon over on the right hand side...
- Following it will let us find the other domains that we're after, e.g., the other Bloomberg domains that share this common POC.
- Let's see what it looks like when we click on the magic link...

# Some Bloomberg-Related Domains We Found This Way

Time Last Seen ↕	Time First Seen ↕	Count ▼	RRName	RRType	RData
2016-02-04 21:58:04	2015-07-24 20:41:05	4711766	businessweek.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307 1251 28800 3600 604800 86400
2019-11-27 18:35:37	2015-02-27 20:17:27	4056438	184.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201022 0906 10800 3600 2592000 172800
2019-12-24 06:42:01	2019-12-20 07:54:04	3524498	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307 3691 43200 3600 3600000 14400
2016-03-24 01:42:22	2015-02-27 20:11:25	2947245	191.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307 3024 72000 3600 3600000 3600
2020-01-11 06:11:55	2019-12-24 06:04:57	2887599	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307 3692 43200 3600 3600000 14400
2019-12-02 12:02:21	2016-06-27 22:11:23	2362435	bloom.bg.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307 0905 10800 3600 2592000 86400
2015-06-08 22:57:39	2015-02-27 20:11:48	1969014	businessweek.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 201307 1246 28800 3600 604800 86400



# Lot of Results? You May Want to "export as CSV"

C	D	E	F	G	I	J
time_last	time_first	count	rname	rrtype	rdata	
1454623084	1437770465	4711766	businessweek.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013071251 28800 3600 604800 86400	
1574879737	1425068247	4056438	184.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010220906 10800 3600 2592000 172800	
1577169721	1576828444	3524498	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073691 43200 3600 3600000 14400	
1458783742	1425067885	2947245	191.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073024 72000 3600 3600000 3600	
1578723115	1577167497	2887599	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073692 43200 3600 3600000 14400	
1575288141	1467065483	2362435	bloom.bg.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013070905 10800 3600 2592000 86400	
1494418438	1447366869	2039564	bwbx.io.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2161338263 28800 3600 604800 600	
1433804259	1425067908	1969014	businessweek.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013071246 28800 3600 604800 86400	
1574879715	1425068570	1955074	185.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010220905 10800 3600 2592000 172800	
1534191169	1480346042	1873040	bloomberght.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2 43200 3600 3600000 86400	
1574879686	1425068348	1816626	186.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010120906 10800 3600 2592000 172800	
1574879719	1425068001	1712096	190.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010120907 10800 3600 2592000 172800	
1574879655	1425068181	1690758	189.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010220905 10800 3600 2592000 172800	
1574879514	1425068826	1670202	188.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010220906 10800 3600 2592000 172800	
1557267379	1556136094	1644865	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073587 43200 3600 3600000 14400	
1424817686	1418946649	1574392	businessweek.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013071242 28800 3600 604800 86400	
1602111358	1579801808	1572954	184.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2010220910 10800 3600 2592000 172800	
1540497417	1525983135	1550690	191.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073083 72000 3600 3600000 3600	
1540326085	1458829390	1550131	43.160.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2012042407 72000 3600 3600000 259200	
1497904617	1487967973	1326407	191.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073065 72000 3600 3600000 3600	
1575288247	1540326187	1305708	43.160.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2012042408 72000 3600 3600000 259200	
1542230248	1537475961	1257577	bloomberg.net.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013080998 1800 3600 3600000 10800	
1547588016	1509737301	1240187	btrd.net.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2011071826 43200 3600 3600000 86400	
1467065529	1425067783	1221069	bloom.bg.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013070904 10800 3600 2592000 86400	
1468957945	1435090859	1137104	bloombergmedia.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013070913 43200 3600 3600000 86400	
1554232479	1553117782	1103967	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073579 1800 3600 3600000 14400	
1596611942	1595397698	1074348	bloomberg.com.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073743 43200 3600 3600000 14400	
1602108311	1554762605	1070350	57.22.208.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2012022102 7200 3600 3600000 1200	
1548447621	1540844655	1046406	191.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073085 72000 3600 3600000 3600	
1565951556	1559265063	1008935	191.69.in-addr.arpa.	SOA	pdns1.ultradns.net. dnsmaster.bloomberg.com. 2013073090 72000 3600 3600000 3600	

# Rdata TXT Search Example



## Another Rdata Example: Using TXT Records to Find Linkages

- We've already looked at an SOA Rdata example.
- Now let's try a second example, this time searching TXT record Rdata.
- To make this work, we'll need to find some interesting bit of information that's common to TXT records of interest.
- Sometimes there may be a common thread we can find and exploit, other times there may not be.
- For this example, while looking at the Malwarebytes Lab Threat Center, (see <https://blog.malwarebytes.com/threats/> ) we noticed the domain `allmygoodlife[dot]com` (defanged here to provide any accidental visits)
- <https://blog.malwarebytes.com/detections/allmygoodlife-com/> says that they list that domain because it has been "associated with malvertising."

# Let's Look At That Domain's TXT Record in DNSDB

The screenshot shows the DNSDB search interface. At the top, there are tabs for 'Flexible Search', 'Standard Search' (highlighted with a red box), and 'Recent Queries'. To the right are links for 'USER GUIDE' and 'DEV DOCS'. Below the tabs, there are two main sections: 'RRSet' (highlighted with a red box) and 'RData'. Under 'RRSet', there are input fields for 'Domain' (containing 'allmygoodlife.com', highlighted with a red box) and 'Bailiwick' (containing 'example.com'). To the right of these fields are 'Limit' (set to 'Max') and 'Offset' (set to '0') dropdowns. Below these are expandable sections for 'Time Fencing (UTC)' and 'Options'. Under 'RData', there is a 'Record Type' dropdown set to 'TXT' (highlighted with a red box). A large green 'SEARCH' button is centered below the input fields. Below the search button, a green banner displays the message: 'Successful Query for: RRSet allmygoodlife.com TXT (Limit 50000)' (highlighted with a red box). Below the banner, there is a 'Show' dropdown set to '10' entries. To the right are buttons for 'EXPORT AS CSV' and 'EXPORT AS JSON'. Below this is a table with the following columns: 'Time Last Seen', 'Time First Seen', 'Count', 'Bailiwick', 'RRName', 'RRType', and 'RData' (highlighted with a red box). The table contains one row of data: '2019-07-12 13:26:16', '2019-07-12 13:26:16', '2', 'allmygoodlife.com.', 'allmygoodlif e.com.', 'TXT', and '"v=spf1 a mx ip4: 159.203.113.141 ~all"'. Below the table, it says '1 to 1 of 1 Results' and there are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

## What's In That TXT Record?

- That TXT record specifies the allowed email senders for that domain using the SPF protocol, see [https://en.wikipedia.org/wiki/Sender\\_Policy\\_Framework](https://en.wikipedia.org/wiki/Sender_Policy_Framework).
- SPF TXT records define the sending FQDNs and IP addresses, ranges, or CIDR netblocks that are allowed to emit email on behalf of a given domain. SPF records can be crafted to enable 3<sup>rd</sup> party Email Service Providers to send email on behalf of a given domain.
- Can we find other records that share the exact same SPF record?
- If so, they MAY be related to our original "clue" or "starting point" domain.
- Let's check... We'll begin with a Flexible Search Regex Search for the SPF record we found.

# Following the Rdata in Flexible Search

Flexible Search | Standard Search | Recent Queries | USER GUIDE | DEV DOCS

Syntax:  Keyword  **Regex**  Globbing ⓘ

Search:  Left-Hand (RRName)  **Right-Hand (RData)** ⓘ

Limit: Max ⓘ | Offset: 0 ⓘ

Find \* ⓘ: "v=spf1 a mx ip4:159.203.113.141 ~all"

Exclude ⓘ: Pattern to Exclude

Record Type: TXT ⓘ

SEARCH

Successful Query for: Regex RData "v=spf1 a mx ip4:159.203.113.141 ~all" TXT (Limit 50000)

Show 10 entries | EXPORT AS CSV | EXPORT AS JSON

RRType	RData
TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"

1 to 1 of 1 Results

First | Previous | 1 | Next | Last

**This is it =>** ⓘ

# And Now, After We've Clicked On The Magic Link...

Show 10 entries

EXPORT AS CSV

EXPORT AS JSON

Time Last Seen ↕	Time First Seen ↕	Count	RRName	RRType	RData
2020-10-07 20:03:44	2019-02-11 13:36:02	100	press-here-to-continue.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-07 20:03:19	2019-02-11 13:35:37	58	press2continue.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-07 20:01:59	2019-02-11 13:30:59	50	browser-games2019.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-07 07:07:58	2019-02-11 13:30:17	45	browsergames2019.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-07 07:03:09	2018-07-20 01:05:11	101	fd7qz88ckd.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-06 17:51:42	2019-09-06 11:06:23	56	5ovrmmmoubi71efvatfd.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-06 07:11:47	2019-12-28 13:23:50	18	dadsecz.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-05 21:04:38	2019-12-31 08:33:56	26	padsimz.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-05 21:03:50	2020-01-02 06:42:56	27	padspmz.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"
2020-10-05 21:03:39	2019-12-31 08:37:19	23	padsipz.com.	TXT	"v=spf1 a mx ip4:159.203.113.141 ~all"

1 to 10 of 2,846 Results

First Previous 1 2 3 4 5 6 7 ... 285 Next Last

# Conclusion

# Key Takeaways

- You now know a little about Flexible Search, why we created it and that it's available at no extra cost for most DNSDB API users.
- You now know you can use it to easily find simple strings in names -- or highly precise regular expressions.
- You can use it to search RRnames or Rdata, including some types of Rdata you couldn't previously easily search, such as TXT records and SOAs.
- You've seen how you can synergistically combine Flexible Search queries with Standard DNSDB queries to get full details when you want them.
- And you've learned how to work with DNSDB Scout, so now it's time for YOU to give DNSDB Flexible Search a try! Have fun!



# As You Use Flexible Search, Send Us Feedback, Please!

- **We affirmatively want to hear from you!**
  - Find a bug?
  - Have an idea for a future enhancement?
  - Frustrated by something?
  - Come up with a novel use case?
- **Tell us about it by writing [support@farsightsecurity.com](mailto:support@farsightsecurity.com)**
  - Please note that any feedback or ideas offered to Farsight will be subject to the terms and conditions of your access agreement.

# Thank You!

Questions?

[info@farsightsecurity.com](mailto:info@farsightsecurity.com)

To sign up for a free trial of our API, go to

<https://www.farsightsecurity.com/trial-api/>