Using Maltego with Farsight DNSDB Transforms

Joe St Sauver, Ph.D. (stsauver@fsi.io)
Distinguished Scientist, Farsight Security, Inc.
Contents

I. Introduction

II. Maltego and the Farsight DNSDB Transform Set

III. Understanding The Farsight DNSDB Transform Set

IV. Manually Running One of the Transforms Using Maltego on the Mac

V. Making A Maltego Machine: (DNS Name) --> (IP Address) --> (Related DNS Names Using That Shared IP)

VI. Conclusion

Appendix A. The Farsight Transform Set (Sorted by Input Type, RRset vs. Rdata, Then "Subjectively")

Appendix B. Sample Transform Output

Acknowledgements: Many thanks to Farsight colleagues Ben April and Marc Evans for their contributions to this document.
I. Introduction

One of the most popular tools for visualizing cybersecurity data and exploring data relationships is Maltego (see https://www.paterva.com/web7/).

This write-up will describe how Maltego can be used in conjunction with Farsight’s DNSDB Transform Set to easily leverage passive DNS approaches.
II. Maltego and the Farsight DNSDB Transform Set

We assume that you're already a Farsight DNSDB API customer; if not, see https://www.farsightsecurity.com/order-services/ for information about obtaining a DNSDB API key.

We also assume that you've already installed and activated the Maltego Classic (or the Maltego XL) client. If not, see the Paterva web site mentioned in the Introduction above.

When you launch Maltego Classic, after the initial splash screen, and after you click on the Transforms tab, you'll see a window that looks roughly something like this:

Figure 1. Basic Maltego Starting Screen
To install the DNSDB Maltego Transform Set, select Transforms Hub, scroll down, then roll your mouse over the Farsight Transform Set. Select Install, and then confirm that you want to install the Transform Set. The Transform Set will install. See Figure 2.

**Figure 2. Successful Installation**

When the Transform Set installation finishes, if you check the Transform Hub, you should see:

**Figure 3. The Farsight Transform Set On The Maltego Transforms Hub (Post-Installation)**
Before you can use the Transforms you'll need to install your DNSDB API key. See Figure 4.

Figure 4. Setting the DNSDB API Key For The Transforms

The Critically Important "Number-of-Results" Slider
While you're configuring Maltego settings, you should also strongly consider increasing the maximum number of results returned. If you fail to do this, you may be surprised to find that the result of every query is twelve or fewer results (since 12 is the default number of results returned in Maltego Classic). To reset that limit go to Investigate --> Number of Results, as shown in Figure 5:

Figure 5. Setting the Maximum Number of Results Returned

[Experienced Maltego users may also want to see Appendix A, for an explanation of how the "Number-of-Results" slider impacts back end processing as well as what's ultimately displayed on screen.]

III. Understanding The Farsight DNSDB Transform Set

You're now ready to begin using the Farsight DNSDB Transforms.

Because of how Maltego works, you do NOT have the option of specifying the equivalent of "command line options" in order to customize a small number of query types. Instead, you get a set of 39 "pre-constructed queries" that can be executed on a variety of inputs. The exact queries you can run depend on the input you're starting with (whether that's a Domain, a DNS Name, an Email Address, a URL, etc.).

For convenience, those transforms are listed on the next page, grouped by Input type, then Transform Description.
### Figure 8. The Farsight Transform Set (Grouped by Input Type)

#### Domain: Delegation Point (sample.com) -- 12 Transforms

<table>
<thead>
<tr>
<th>#</th>
<th>Input</th>
<th>Transform Description</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Domain</td>
<td>To records with this hostname</td>
<td>paterva.v2.dnsdbrrsetDomain</td>
</tr>
<tr>
<td>2</td>
<td>Domain</td>
<td>Lookup *.$domain</td>
<td>paterva.v2.dnsdbrrsetwclDomain</td>
</tr>
<tr>
<td>3</td>
<td>Domain</td>
<td>Lookup *.$domain/A</td>
<td>paterva.v2.dnsdbrrsetwclDomainA</td>
</tr>
<tr>
<td>4</td>
<td>Domain</td>
<td>Lookup *.$domain/AAAA</td>
<td>paterva.v2.dnsdbrrsetwclDomainAAAA</td>
</tr>
<tr>
<td>5</td>
<td>Domain</td>
<td>Lookup *.$domain/CNAME</td>
<td>paterva.v2.dnsdbrrsetwclDomainCNAME</td>
</tr>
<tr>
<td>6</td>
<td>Domain</td>
<td>Lookup $domain.*</td>
<td>paterva.v2.dnsdbrrsetwcrDomain</td>
</tr>
<tr>
<td>7</td>
<td>Domain</td>
<td>Lookup $domain.*/A</td>
<td>paterva.v2.dnsdbrrsetwcrDomainA</td>
</tr>
<tr>
<td>8</td>
<td>Domain</td>
<td>Lookup $domain.*/AAAA</td>
<td>paterva.v2.dnsdbrrsetwcrDomainAAAA</td>
</tr>
<tr>
<td>9</td>
<td>Domain</td>
<td>Lookup $domain.*/CNAME</td>
<td>paterva.v2.dnsdbrrsetwcrDomainCNAME</td>
</tr>
<tr>
<td>10</td>
<td>Domain</td>
<td>Lookup NS for this Domain</td>
<td>paterva.v2.dnsdbrrsetDomainNS</td>
</tr>
<tr>
<td>11</td>
<td>Domain</td>
<td>Lookup MX for this Domain</td>
<td>paterva.v2.dnsdbrrsetDomainMX</td>
</tr>
<tr>
<td>12</td>
<td>Domain</td>
<td>To DNSNames with this value</td>
<td>paterva.v2.dnsdbrrdataDomain</td>
</tr>
</tbody>
</table>

#### DNS Name: Fully Qualified Domain Name (e.g., www.sample.com) -- 19 Transforms

<table>
<thead>
<tr>
<th>#</th>
<th>Input</th>
<th>Transform Description</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>DNS Name</td>
<td>To records with this hostname</td>
<td>paterva.v2.dnsdbrrsetDNSName</td>
</tr>
<tr>
<td>14</td>
<td>DNS Name</td>
<td>Lookup *.$dnsname</td>
<td>paterva.v2.dnsdbrrsetwclDNSName</td>
</tr>
<tr>
<td>15</td>
<td>DNS Name</td>
<td>Lookup *.$dnsname/A</td>
<td>paterva.v2.dnsdbrrsetwclDNSNameA</td>
</tr>
<tr>
<td>16</td>
<td>DNS Name</td>
<td>Lookup *.$dnsname/AAAA</td>
<td>paterva.v2.dnsdbrrsetwclDNSNameAAAA</td>
</tr>
<tr>
<td>17</td>
<td>DNS Name</td>
<td>Lookup *.$dnsname/CNAME</td>
<td>paterva.v2.dnsdbrrsetwclDNSNameCNAME</td>
</tr>
<tr>
<td>18</td>
<td>DNS Name</td>
<td>Lookup $dnsname.*</td>
<td>paterva.v2.dnsdbrrsetwcrDNSName</td>
</tr>
<tr>
<td>19</td>
<td>DNS Name</td>
<td>Lookup $dnsname.*/A</td>
<td>paterva.v2.dnsdbrrsetwcrDNSNameA</td>
</tr>
<tr>
<td>20</td>
<td>DNS Name</td>
<td>Lookup $dnsname.*/AAAA</td>
<td>paterva.v2.dnsdbrrsetwcrDNSNameAAAA</td>
</tr>
<tr>
<td>21</td>
<td>DNS Name</td>
<td>Lookup $dnsname.*/CNAME</td>
<td>paterva.v2.dnsdbrrsetwcrDNSNameCNAME</td>
</tr>
<tr>
<td>22</td>
<td>DNS Name</td>
<td>To A Records for this DNSName</td>
<td>paterva.v2.dnsdbrrsetDNSNameToA</td>
</tr>
</tbody>
</table>
### Using Maltego with Farsight DNSDB

<table>
<thead>
<tr>
<th>Transform ID</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.</td>
<td>DNS Name</td>
<td>To AAAA Records for this DNSName</td>
</tr>
<tr>
<td>24.</td>
<td>DNS Name</td>
<td>To TXT Records for this DNSName</td>
</tr>
<tr>
<td>25.</td>
<td>DNS Name</td>
<td>To NS for this DNSName</td>
</tr>
<tr>
<td>26.</td>
<td>DNS Name</td>
<td>To MX for this DNSName</td>
</tr>
<tr>
<td>27.</td>
<td>DNS Name</td>
<td>To SOA Records for this DNSName</td>
</tr>
<tr>
<td>28.</td>
<td>DNS Name</td>
<td>To SRV Records for this DNSName</td>
</tr>
<tr>
<td>29.</td>
<td>DNS Name</td>
<td>Records with this value</td>
</tr>
<tr>
<td>30.</td>
<td>DNS Name</td>
<td>Domains Using This MX</td>
</tr>
<tr>
<td>31.</td>
<td>DNS Name</td>
<td>Domains Using This NS</td>
</tr>
<tr>
<td>32.</td>
<td>Phrase</td>
<td>Lookup <em>.</em>$phrase</td>
</tr>
<tr>
<td>33.</td>
<td>Phrase</td>
<td>lookup $phrase.*</td>
</tr>
<tr>
<td>34.</td>
<td>Phrase</td>
<td>To DNSNames from this IPv6 Address</td>
</tr>
<tr>
<td>35.</td>
<td>Email Address</td>
<td>To DNSNames from this email</td>
</tr>
<tr>
<td>36.</td>
<td>Email Address</td>
<td>MX from E-mail address</td>
</tr>
<tr>
<td>37.</td>
<td>URL</td>
<td>To DNSNames from this URL</td>
</tr>
<tr>
<td>38.</td>
<td>IPv4 Address</td>
<td>To DNSNames with this IP</td>
</tr>
<tr>
<td>39.</td>
<td>Netblock</td>
<td>To DNSNames with this value</td>
</tr>
</tbody>
</table>

**Phrase (Phrases are IPv6 Addresses, CIDR netblocks, and Rdata text you'd like to search) -- 3 Transforms**

- **32. Phrase**: Lookup *.*$phrase
- **33. Phrase**: lookup $phrase.*
- **34. Phrase**: To DNSNames from this IPv6 Address

**Email Address (joe@sample.com) -- 2 Transforms**

- **35. Email Address**: To DNSNames from this email
- **36. Email Address**: MX from E-mail address

**Other (Note: Netblocks look like a.b.c.d-e.f.g.h, NOT CIDR netblocks (see "Phrase" above for CIDRs)) -- 3 Transforms**

- **37. URL**: To DNSNames from this URL
- **38. IPv4 Address**: To DNSNames with this IP
- **39. Netblock**: To DNSNames with this value

---

**Sample output for each of the 39 defined Farsight transforms from Figure 8 can be seen in Appendix B.**

**An Aside: Decoding The “Name” Column From Figure 8**
(1) Note that all of the transforms begin with the invariant string "paterva.v2.dnsdb". You can normally mentally "tune that part out."

(2) Next, you'll see either "rrset" ("left hand side" of a DNS record), or "rdata" ("right hand side" of a DNS record). [for more on the difference between rrsets and rdata see please see the blog post that's at https://www.farsightsecurity.com/2015/03/11/stsauver-rrset-rdata/]

(3) You may then sometimes see reference to "wcl" (wildcard left hand side, e.g., *.example.com), or "wcr" wildcard right hand side (e.g., example.*).

(4) Next you'll normally see a reference to a Maltego Entity such as "DNS Name", "Phrase", "URL", "Netblock", etc. All Maltego Entities are defined in, and can be reviewed in, the Maltego Entity Manager.

Paterva also has excellent documentation available online. See for example:

- https://docs.paterva.com/en/entity-guide/standard_entities/infrastructure/Domain/ (e.g., delegation point, effective 2nd-level domain)
- https://docs.paterva.com/en/entity-guide/standard_entities/infrastructure/DNSName/ (e.g., FQDN, hostname)

While "Phrase" normally equals "any text or part thereof," in the case of the Farsight Transforms, "Phrase" is used as a "data type of last resort" to handle elements which don't have a more specific data type available. This includes things like IPv6 addresses and CIDR netblocks. "Phrase" is also used as a way to query Rdata values found in TXT records.

(5) After that, the Transform name may specify a subset of possible DNS record types, e.g., MX, SRV, TXT, etc.

**Note:** We're also aware that some Transforms may seem to be "duplicative" (for example "Lookup *.$domain", "Lookup *.$phrase", and "Lookup *.$dnsname").

Please note that in this case, while their naming seems similar, the entities they work on (and allow as inputs) are different.
IV. Manually Running One of the Transforms

We'll now show you an example of manually invoking one of the Transforms.

We assume you have installed Maltego on a Mac (Maltego on a Windows 10 system will be similar once the application has been started, except for things like file paths).

(1) If Maltego isn't already running, start Maltego by double clicking on the Maltego icon in /Applications. After splash screens, you should see a screen that looks approximately like Figure 9:

Figure 9. Initial Maltego Screen

If you don't have a "New Graph" panel open as part of your Maltego display, click on the little "Page +" icon that's immediately to the right of the "bowling ball" icon in the upper left hand corner.
(2) Now click and drag the "DNS Name" Entity from the "Entity Palette" in the left column over into the main white "New Graph" panel. You should see something like what's shown in Figure 10.

Figure 10. Maltego With DNS Name Entity dragged onto the New Graph panel.

(3) The default name that's displayed (alpine.paterva.com) is NOT the name we're interested in, so double click on it and type in a different name. For this example, let's put in www.reed.edu. After typing in that DNS Name, hit return. The result should look like Figure 11.

Figure 11. DNS Name Entity Now Showing The Name of Interest
(4) Now need to decide which Transform we want to run on that Entity. Hold down the Control key and click on the Entity to see what transforms are available for the sort of Entity we're using. See Figure 12.

**Figure 12. Picking a Transform**

We choose “To A Records for this DNSName” and click the right triangular arrow to the right of that item to execute that Transform.

**Figure 13. Result of Running That Transform**

**Note:** Many different output formats are available, see the "View" menu to the left of the graph. If you prefer tables to diagrams, in particular, be sure to check out the tabular view.
available from the View menu.

Also Note: If you look at the default table view, and wish you could suppress some of those columns, note that you CAN do so. After selecting table view, click on "select columns" icon (the little mesh grid) on the far right hand of the Type/Headings/etc. row just above the actual rows of data) and select just the columns you want.

(5) We can now "chain" from our initial results to see what DNSNames (if any) also share that IP. In this case, the only Transform available to us is "To DNSNames with this IP" which makes our choice of Transform rather straightforward. See Figure 14.

Figure 14. Checking To See If Any Other DNS Names Share That IP Address

After clicking on the right triangular arrow next to the Transform name, the Transform runs, producing the result shown in Figure 15.
Figure 15. Results From Running The "To DNSnames with this IP" Transform

Clearly results were found, but we can’t currently see them.

We’ll close some of the panels we don’t currently need, resize the "New Graph" window, and click on the magnifying glass at the top of the screen to "zoom to fit" the output. See Figure 16.

Figure 16. Output From Our Transforms, More Readily Visible Now
(6) Sometimes you may just prefer a list of results to a diagram. If so, change that in the View menu to the left of the New Graph panel. See Figure 17. Note that the right-most column shows the number of hits that DNSDB has seen for each row.

*Figure 17. List View of Results*

You can experiment with other views, too, obviously.

(7) If your analysis is concluded, you may want to save your results.

There are multiple things you can save:

- You can save your Maltego session (so you can easily resume your analysis where you left off).

  To save your session, click on the floppy disk icon near the top edge of the Maltego window (or go to the circle icon in the upper left corner and select Save).

- You can export a copy of the Maltego graph by going to "Import | Export" --> "Export Graph as Image."

  You’ll need to pick a name and location for the graph you’re about to export, as well as a format (such as JPEG). You can see a sample exported graph in Figure
You can also export a copy of the "raw data" you've found as an Excel Spreadsheet file, or as a comma separated variable (CSV) file, by going to "Import | Export" --> "Export Graph To Table."

You'll need to pick a name and location for the graph you're about to export, as well as a format (such as CSV). You can see a sample exported table in Figure 19, below.
Using Maltego with Farsight DNSDB

**Figure 18. Sample Exported Graph**

![Graph showing connections between IP addresses and domain names.]

**Figure 19. Sample Exported-as-CSV Table Data**

134.10.2.252,alumni.reed.edu  
134.10.2.252,comradesofthequest.com  
134.10.2.252,comradesofthequest.org  
134.10.2.252,nwacc.org  
134.10.2.252,nwacc.reed.edu  
134.10.2.252,reed.edu  
134.10.2.252,web.reed.edu  
134.10.2.252,www.reed.edu  
www.reed.edu,134.10.2.252

Copyright © 2018 Farsight Security, Inc. All trademarks are properties of their respective owners.
V. Making A Maltego Machine:
(DNS Name) --> (IP Address) --> (Related DNS Names Using That Shared IP Address)

In addition to manually running individual Transforms, you can also create a Maltego "Machine" that will run a "pipeline" of Transforms. For example, we can create a Maltego Machine to run the two Transforms we just manually ran for www.reed.edu, making it easy to do that same run for other DNS Names.

(1) Begin by going to Machines --> New Machine, then supply configuration details.

Figure 20. Make a New Machine In Maltego
Figure 21. Supply configuration details

Complete the initial Machine by choosing its type, as shown in Figure 22:

Figure 22. Choose the Type of Machine
(2) You’re now ready to customize the skeletal Machine outline you’ll be given. We’ll end up with what’s shown in Figure 23.

*Figure 23. Our Sample Machine’s Simple Code*
(3) After saving our machine, we can then run it. See Figure 24.

*Figure 24. Picking the Machine We Want to Start*

We also need to provide the name we want to run the Machine on... as a test, let's do www.reed.edu again.

*Figure 25. The Target DNS Name For Our Machine*

When we click Finish, the Machine will begin to run. See the output in Figure 26.
This output should look familiar (e.g., from when we ran these same transforms manually, earlier in this write-up).

Note that just as when running Transforms manually, when you’re running a Maltego Machine you may need to rearrange or close panels, scroll, or use Investigate--> (magnifying glass) [aka “Zoom to Fit”] to see portions of your results.

Caution: Note that Machines which perform "chained queries" may potentially end up consuming multiple DNSDB queries from your quota every time they’re run.

For example, assume you construct a Machine that finds all domains that use a given name server, and then the Machine is programmed to look up each of those domains individually. Such a Machine could consume hundreds or even thousands of queries or more depending on the popularity/usage of that name server.
VI. Conclusion

Maltego is a very popular framework for conducting cyber forensic investigations and doing other data mining.

You’ve now seen how you can easily use Farsight Security's DNSDB with Maltego as part of your investigations.

In this write-up you’ve learned:

- How to install the Farsight Transform Set for Maltego
- How to configure the Transforms with your DNSDB API key
- How to decode the Farsight Transform's naming convention
- How to manually run the Transforms upon an Entity
- How to save/export the results of your analysis
- How to create and run a Maltego Machine to automate that process

We hope that Maltego DNSDB users have found this write up helpful.

If you have any feedback, please feel free to drop us a note to share your thoughts at support@fsi.io
Appendix A.

A Subtle But Critically Important "Side Effect" of The "Number-of-Results" Slider...

The "Number-of-Results" slider controls the number of results displayed in a Maltego graph -- that's well understood and as expected.

What may be less well understood is the fact that the "Number-of-Results" slider ALSO shapes backend processing that's done by the Farsight DNSDB Transforms PRIOR TO results getting displayed.

To understand the implications of this, consider the "Lookup *.Domain" Transform. If we have the Number-of-Results slider set to 256, and run the Transform on uoregon.edu, we see a graph that looks like Figure 6:

Figure 6: "Lookup *.Domain" Output With Number-of-Results Set to 256
We would normally expect to see MANY results in that graph, not just the two results shown. So what happened?

The answer can be seen by a careful inspection of the Maltego "Details" Window. To check it out, click on the uoregon.edu node near the bottom right portion of the graph shown in the Graph Window, then go to Windows --> Detail View. You should see something that looks like Figure 7:

*Figure 7. Details View For One Output Node, Lookup *.$domain, for the case of "uoregon.edu"*
In this case, there are LOTS of results from DNSDB that all have the same left hand side (all are "uoregon.edu"). Those results get condensed for display purposes, and end up getting shown as just one (1) uoregon.edu node in the Maltego graph.

Unfortunately, there are so many results that get "used up" that way, other unique/more interesting domains won't end up getting displayed if the Maltego transform is run with a small "Number of Results" slider setting.

**Q. ‘Why Not Just Ignore The "Number of Results" Slider When Accumulating/Aggregating Results?’**

A. While we could just "brute force" the processing and collect up to a million results for each step of the DNSDB Transform's analysis, doing so will normally be a waste of time and effort if we're ultimately only going to ultimately display just 12 or 50 or 256 results.

That's why Farsight set the internal Transform-related processing limit to be an order of magnitude higher than the specified output.

That said, if you encounter issues with "SOA pollution" or similar dreck in the "Lookup *. $Domain" Transform, you may want to consider the alternative "Lookup *. $Domain/A"
Using Maltego with Farsight DNSDB

Transform that will JUST return "A" records,¹ or leave the "Number of Results" slider set to return the maximum number of results.

---

¹ See also the "Lookup *.Domain/AAAA" Transform that will JUST return IPv6 "quad A" records, and the "Lookup *.Domain/CNAME" Transform that will JUST return CNAME records, too.
Appendix B.

Sample Transforms

*Note: The numbering of the Transforms in this appendix correspond to the numbers from Figure 8.*

1. "To records with this hostname"

Name: paterva.v2.dnsdbrrsetDomain
Input Type: Domain
Input: fsi.io
2. "Lookup *.\$domain"

Name: paterva.v2.dnsdbrrsetwclDomain
Input Type: Domain
Input: willamette.edu
Only selected columns shown
3. "Lookup *.$domain/A"

Name: paterva.v2.dnsdbrrsetwclDomainA
Input Type: Domain
Input: willamette.edu
Only selected columns shown
4. "Lookup *.$domain/AAAA"

Name: paterva.v2.dnsbrrsetwclDomainAAAA
Input Type: Domain
Input: uoregon.edu
Only selected columns shown
5. "Lookup *.$domain/CNAME"

Name: paterva.v2.dnsbrrsetwclDomainCNAME
Input Type: Domain
Input: uoregon.edu
Only selected columns shown
6. "Lookup $domain."

Name: paterva.v2.dnsbrrsetwcrDomain
Input Type: Domain
Input: uoregon
Only selected columns shown

Note: Input to this Transform may not be (strictly speaking) a complete and valid domain per se.
7. "Lookup $domain./A"

Name: paterva.v2.dnsbrrsetwcrDomainA
Input Type: Domain
Input: uoregon
Only selected columns shown

Note: Input to this Transform may not be (strictly speaking) a complete and valid domain per se.
8. "Lookup $domain.*/AAAA"

Name: paterva.v2.dnsdbrrsetwcrDomainAAAA
Input Type: Domain
Input: uoregon

Note: Input to this Transform may not be (strictly speaking) a complete and valid domain per se.
9. "Lookup $domain./CNAME"

Name: paterva.v2.dnsdbrrsetwcrDomainCNAME
Input Type: Domain
Input: uoregon

Note: Input to this Transform may not be (strictly speaking) a complete and valid domain per se.
10. "Lookup NS for this Domain"

Name: paterva.v2.dnsdbrrsetDomainNS
Input Type: Domain
Input: reed.edu
11. "Lookup MX for this Domain"

Name: paterva.v2.dnsdbrrsetDomainMX
Input Type: Domain
Input: ucla.edu
12. "To DNSNames with this value"

Name: paterva.v2.dnsdbrdomain
Input Type: Domain
Input: ietf.org
13. "To records with this hostname"

Name: paterva.v2.dnsbrrsetDNSName
Input Type: DNS Name
Input: www.fsi.io
14. "Lookup *.\$dnsname"

Name: paterva.v2.dnsdbrrsetwclDNSName
Input Type: DNS Name
Input: cs.uoregon.edu

**NOTE:** DO NOT INCLUDE THE LEADING ASTERISK AND DOT IN THE SUPPLIED INPUT
15. "Lookup *.\$dnsname/A"

Name: paterva.v2.dnsbrrsetwclDNSNameA  
Input Type: DNS Name  
Input: cs.uoregon.edu

NOTE: DO NOT INCLUDE THE LEADING ASTERISK AND DOT IN THE SUPPLIED INPUT
16. "Lookup *.$dnsname/AAAA"

Name: paterva.v2.dnsdbrrsetwclDNSNameAAAA
Input Type: DNS Name
Input: cs.uoregon.edu
List view with some columns deleted.

**NOTE:** DO NOT INCLUDE THE LEADING ASTERISK AND DOT IN THE SUPPLIED INPUT
17. "Lookup *.,$dnsname/CNAME"

Name: paterva.v2.dnsbrrsetwclDNSNameCNAME
Input Type: DNS Name
Input: uoregon.edu

NOTE: DO NOT INCLUDE THE LEADING ASTERISK AND DOT IN THE SUPPLIED INPUT
18. "Lookup $dnsname.*"

Name: paterva.v2.dnsbrrsetwcrDNSName
Input Type: DNS Name
Input: uoregon

**NOTE:** **DO NOT** INCLUDE THE TRAILING DOT AND ASTERISK IN THE SUPPLIED INPUT
19. "Lookup $dnsname.*/A"

Name: paterva.v2.dnsdbrrsetwcrDNSNameA
Input Type: DNS Name
Input: uoregon

NOTE: DO NOT INCLUDE THE TRAILING DOT AND ASTERISK IN THE SUPPLIED INPUT
20. "Lookup $dnsname.*/AAAA"

Name: paterva.v2.dnsdbrrsetwcrDNSNameAAAA
Input Type: DNS Name
Input: uoregon

**NOTE: DO NOT INCLUDE THE TRAILING DOT AND ASTERISK IN THE SUPPLIED INPUT**
21. "Lookup $dnsname./CNAME"

Name: paterva.v2.dnsdbrrsetwcrDNSNameCNAME
Input Type: DNS Name
Input: uoregon

NOTE: DO NOT INCLUDE THE TRAILING DOT AND ASTERISK IN THE SUPPLIED INPUT
22. "To A Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToA
Input Type: DNS Name
Input: phloem.uoregon.edu
23. "To AAAA Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToAAAA
Input Type: DNS Name
Input: phloem.uoregon.edu
24. "To TXT Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToTXT
Input Type: DNS Name
Input: *.fsi.io
25. "To NS for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToNS
Input Type: DNS Name
Input: www.ucla.edu
26. "To MX for this DNSName"

Name: paterva.v2.dnsbrrsetDNSNameToMX
Input Type: DNS Name
Input: ucla.edu
27. "To SOA Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToSOA
Input Type: DNS Name
Input: ucla.edu
28. "To SRV Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToSRV
Input Type: DNS Name
Input: *.fsi.io
29. "Records with this value"

Name: paterva.v2.dnsdbrdatalDNSName
Input Type: DNS Name
Input: phloem.uoregon.edu
Results limited to no more than 50 results for the purposes of this example
30. "Domains Using This MX"

Name: paterva.v2.dnsdbrdataMXType
Input Type: DNS Name
Input: microsoft-com.mail.protection.outlook.com
Limited to: MX records
List view
31. "Domains Using This NS"

Name: paterva.v2.dnsdbrdataNSType
Input Type: DNS Name
Input: phloem.uoregon.edu
Limited to: NS records
Number of results set to 256 (there were more than that in this case)
List view
Only selected columns shown

32. "Lookup *.phrase"
Name: paterva.v2.dnsdbrrsetwclPhrase
Input Type: Phrase
Input: eou.edu
Only selected columns shown
Using Maltego with Farsight DNSDB

33. "lookup $phrase."

Name: paterva.v2.dnsdbrrsetwcrPhrase
Input Type: Phrase
Input: www.ibm
34. "To DNSNames from this IPv6 Address"

Name: paterva.v2.dnsdbrdatalPV6Address
Input Type: Phrase
Input: 2400:cb00:2048:1::6814:155
35. "To DNSNames from this email"

Name: paterva.v2.dnsdbrrsetEmail
Input Type: Email address
Input: stsauver@fsi.io
36. "MX from E-mail address"

Name: paterva.v2.dnsdbrrsetEmailMX
Input Type: Email address
Input: stsaucer@fsi.io
Results limited to no more than 12 results for the purposes of this example
37. "To DNSNames from this URL"

Name: paterva.v2.dnsdbrrsetURL
Input Type: URL
Input: https://www.ieee.org/
38. "To DNSNames with this IP"

Name: paterva.v2.dnsdbrdatalIPv4Address
Input Type: IPv4 Address
Input: 128.223.32.35
39. "To DNSNames with this value"

Name: paterva.v2.dnsdbdataNetblock
Input Type: Netblock
Input: 128.223.32.0-128.223.32.255

IPv6 netblocks or CIDR netblocks are phrases, not "netblocks" at this point in time.