

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

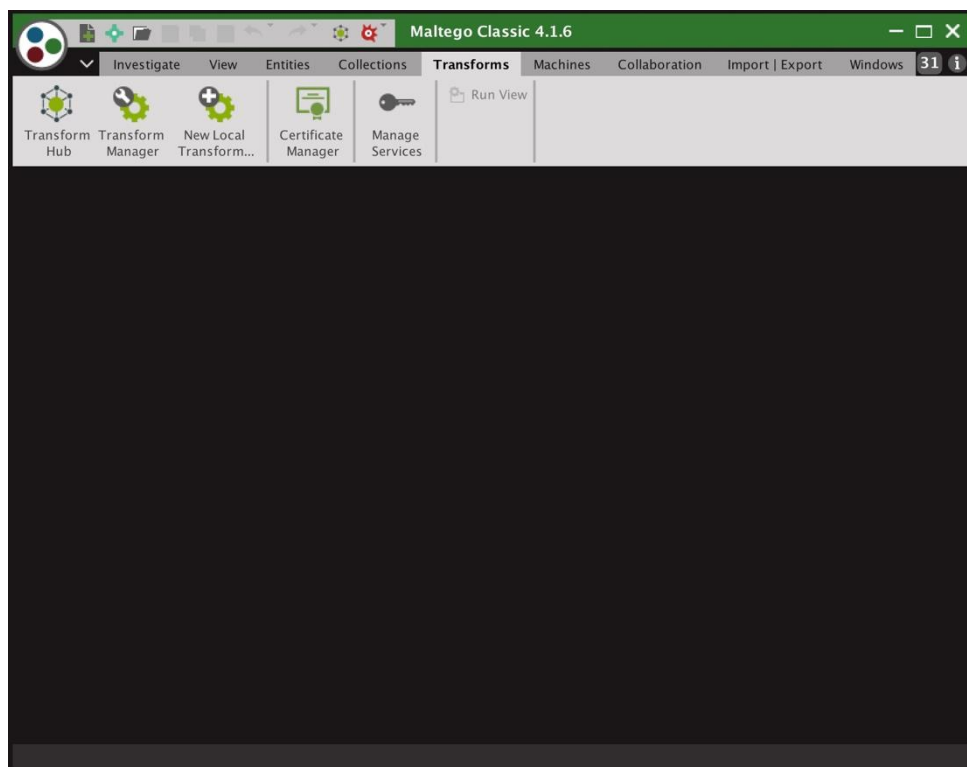
We assume that you're already a Farsight DNSDB API customer; if not, see <https://www.farsightsecurity.com/order-services/> for information about obtaining a DNSDB API key.

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.

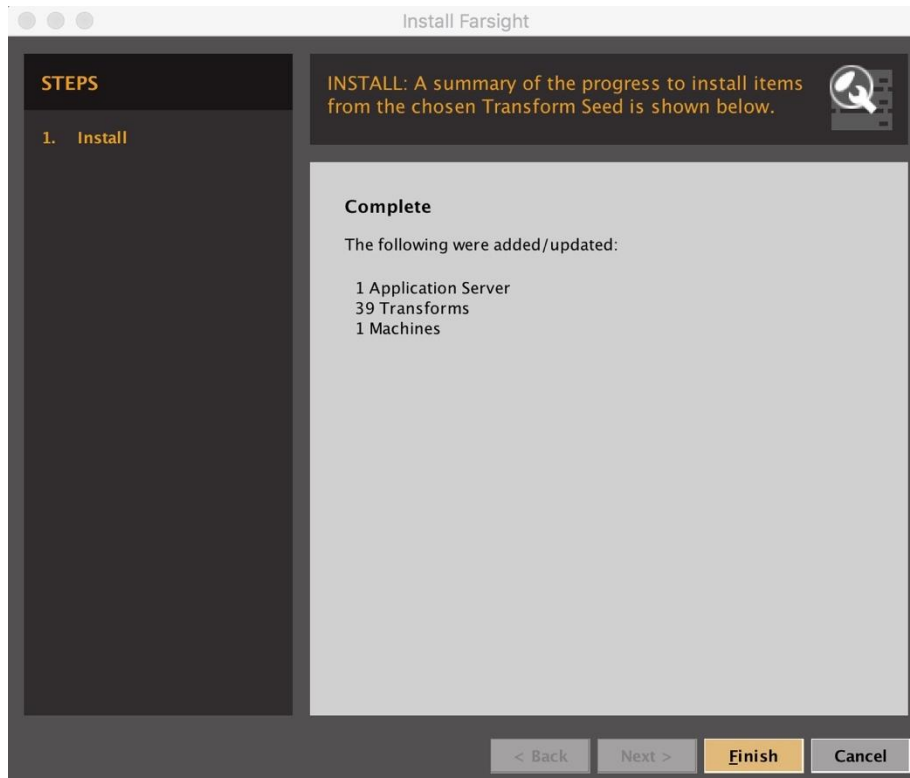
When you launch Maltego Classic, after the initial splash screen, and after you click on the Transforms tab, you'll see a window that looks roughly something like this:

Figure 1. Basic Maltego Starting Screen



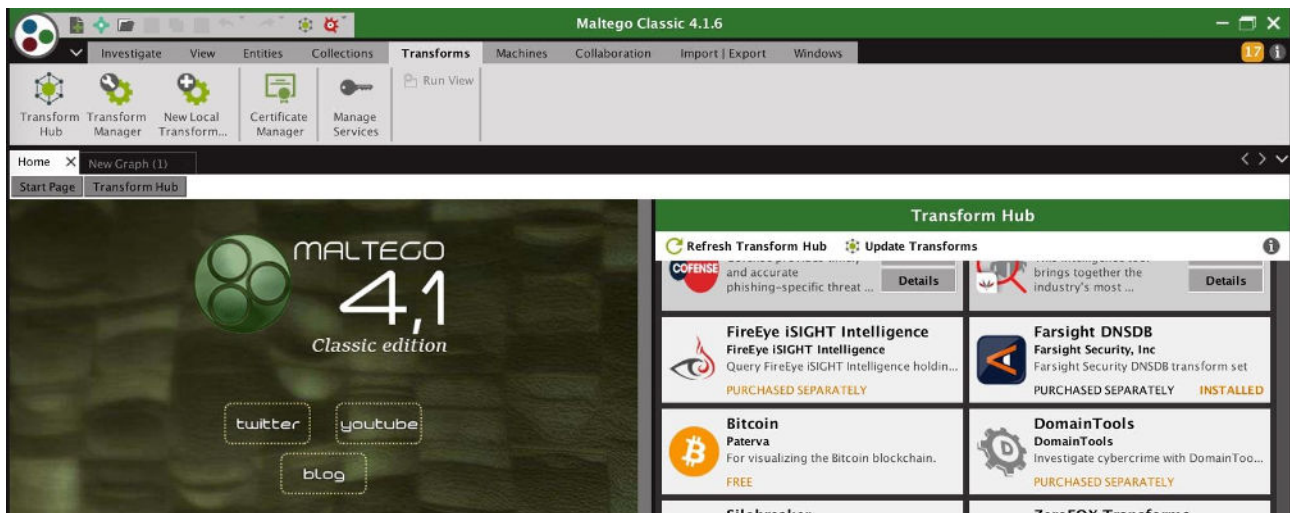
To install the DNSDB Maltego Transform Set, select Transforms Hub, scroll down, then roll your mouse over the Farsight Transform Set. Select Install, and then confirm that you want to install the Transform Set. The Transform Set will install. See Figure 2.

Figure 2. Successful Installation



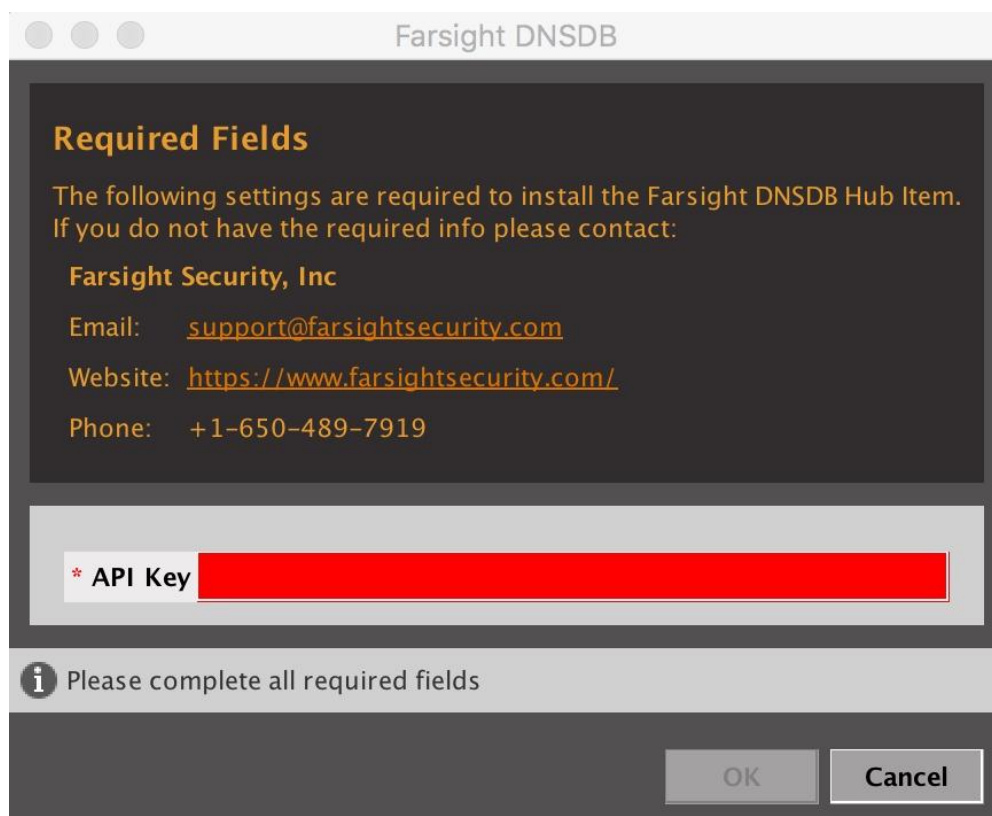
When the Transform Set installation finishes, if you check the Transform Hub, you should see:

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.

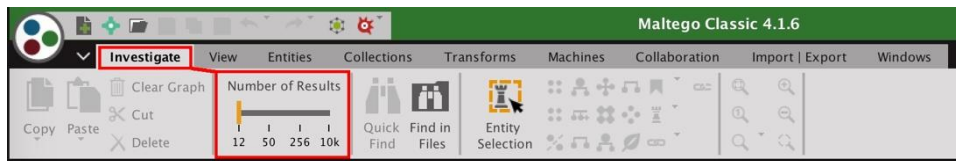
Figure 4. Setting the DNSDB API Key For The Transforms



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)

#	Input	Transform Description	Name
Domain: Delegation Point (sample.com) -- 12 Transforms			
1.	Domain	To records with this hostname	paterva.v2.dnsdbrrsetDomain
2.	Domain	Lookup *.\$domain	paterva.v2.dnsdbrrsetwclDomain
3.	Domain	Lookup *.\$domain/A	paterva.v2.dnsdbrrsetwclDomainA
4.	Domain	Lookup *.\$domain/AAAA	paterva.v2.dnsdbrrsetwclDomainAAAA
5.	Domain	Lookup *.\$domain/CNAME	paterva.v2.dnsdbrrsetwclDomainCNAME
6.	Domain	Lookup \$domain.*	paterva.v2.dnsdbrrsetwcrDomain
7.	Domain	Lookup \$domain.* /A	paterva.v2.dnsdbrrsetwcrDomainA
8.	Domain	Lookup \$domain.* /AAAA	paterva.v2.dnsdbrrsetwcrDomainAAAA
9.	Domain	Lookup \$domain.* /CNAME	paterva.v2.dnsdbrrsetwcrDomainCNAME
10.	Domain	Lookup NS for this Domain	paterva.v2.dnsdbrrsetDomainNS
11.	Domain	Lookup MX for this Domain	paterva.v2.dnsdbrrsetDomainMX
12.	Domain	To DNSNames with this value	paterva.v2.dnsdbrrsetDomain

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

13.	DNS Name	To records with this hostname	paterva.v2.dnsdbrrsetDNSName
14.	DNS Name	Lookup *.\$dnsname	paterva.v2.dnsdbrrsetwclDNSName
15.	DNS Name	Lookup *.\$dnsname/A	paterva.v2.dnsdbrrsetwclDNSNameA
16.	DNS Name	Lookup *.\$dnsname/AAAA	paterva.v2.dnsdbrrsetwclDNSNameAAAA
17.	DNS Name	Lookup *.\$dnsname/CNAME	paterva.v2.dnsdbrrsetwclDNSNameCNAME
18.	DNS Name	Lookup \$dnsname.*	paterva.v2.dnsdbrrsetwcrDNSName
19.	DNS Name	Lookup \$dnsname.* /A	paterva.v2.dnsdbrrsetwcrDNSNameA
20.	DNS Name	Lookup \$dnsname.* /AAAA	paterva.v2.dnsdbrrsetwcrDNSNameAAAA
21.	DNS Name	Lookup \$dnsname.* /CNAME	paterva.v2.dnsdbrrsetwcrDNSNameCNAME
22.	DNS Name	To A Records for this DNSName	paterva.v2.dnsdbrrsetDNSNameToA

23.	DNS Name	To AAAA Records for this DNSName	paterva.v2.dnsdbrrsetDNSNameTo AAAA
24.	DNS Name	To TXT Records for this DNSName	paterva.v2.dnsdbrrsetDNSNameTo TXT
25.	DNS Name	To NS for this DNSName	paterva.v2.dnsdbrrsetDNSNameTo NS
26.	DNS Name	To MX for this DNSName	paterva.v2.dnsdbrrsetDNSNameTo MX
27.	DNS Name	To SOA Records for this DNSName	paterva.v2.dnsdbrrsetDNSNameTo SOA
28.	DNS Name	To SRV Records for this DNSName	paterva.v2.dnsdbrrsetDNSNameTo SRV
29.	DNS Name	Records with this value	paterva.v2.dnsdbrrdata DNSName
30.	DNS Name	Domains Using This MX	paterva.v2.dnsdbrrdata MXType
31.	DNS Name	Domains Using This NS	paterva.v2.dnsdbrrdata NSType

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

32.	Phrase	Lookup *.\$phrase	paterva.v2.dnsdbrrsetwcl Phrase
33.	Phrase	lookup \$phrase.*	paterva.v2.dnsdbrrsetwcr Phrase
34.	Phrase	To DNSNames from this IPv6 Address	paterva.v2.dnsdbrrdata IPv6Address

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

35.	Email Address	To DNSNames from this email	paterva.v2.dnsdbrrset Email
36.	Email Address	MX from E-mail address	paterva.v2.dnsdbrrset EmailMX

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	paterva.v2.dnsdbrrset URL
38.	IPv4 Address	To DNSNames with this IP	paterva.v2.dnsdbrrdata IPv4Address
39.	Netblock	To DNSNames with this value	paterva.v2.dnsdbrrdata Netblock

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)
- https://docs.paterva.com/en/entity-guide/standard_entities/personal/Phrase/

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.

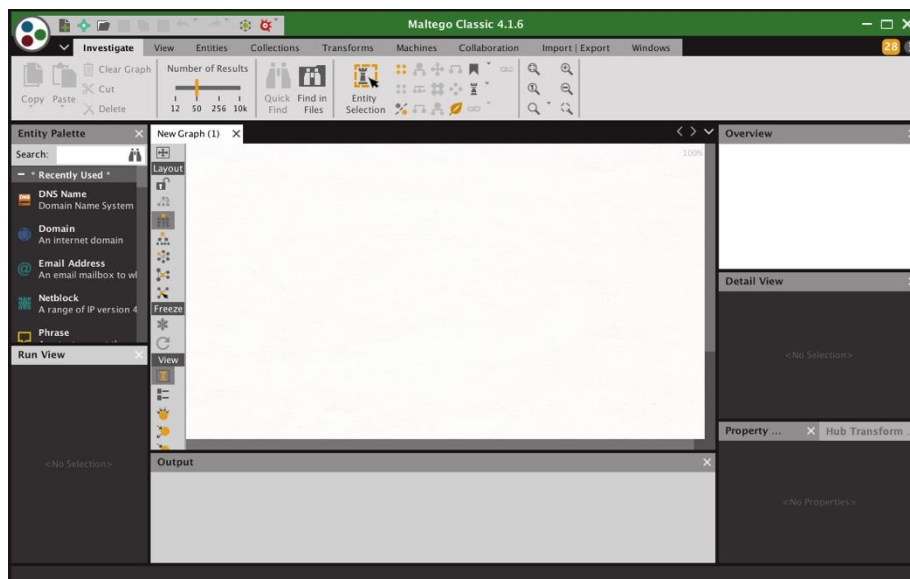
IV. Manually Running One of the Transforms

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:

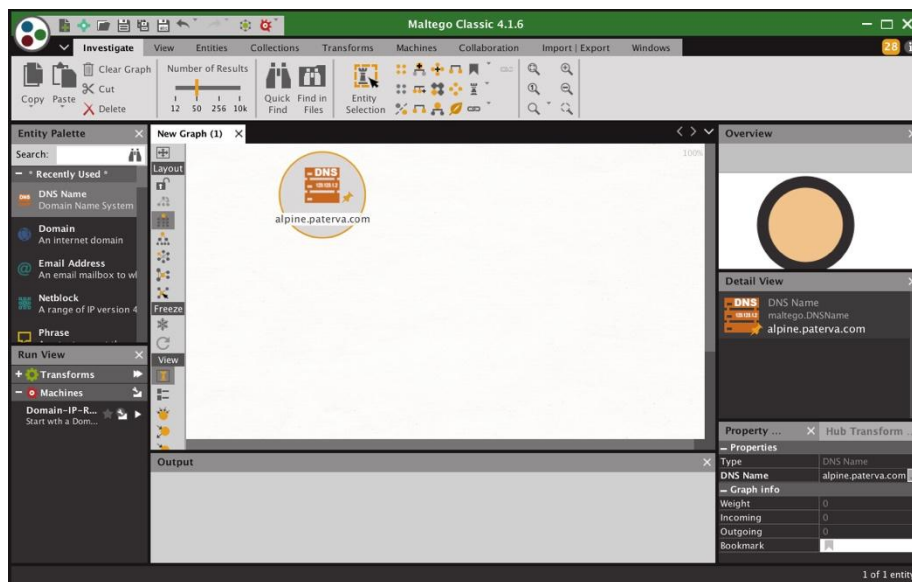
Figure 9. Initial Maltego Screen



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.

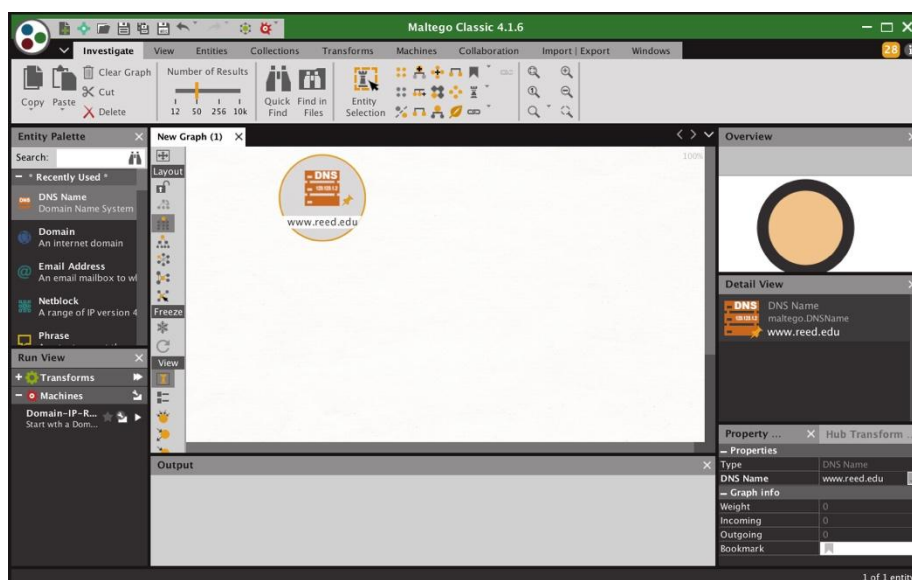
(2) Now click and drag the "DNS Name" Entity from the "Entity Palette" in the left column over into the main white "New Graph" panel. You should see something like what's shown in Figure 10.

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



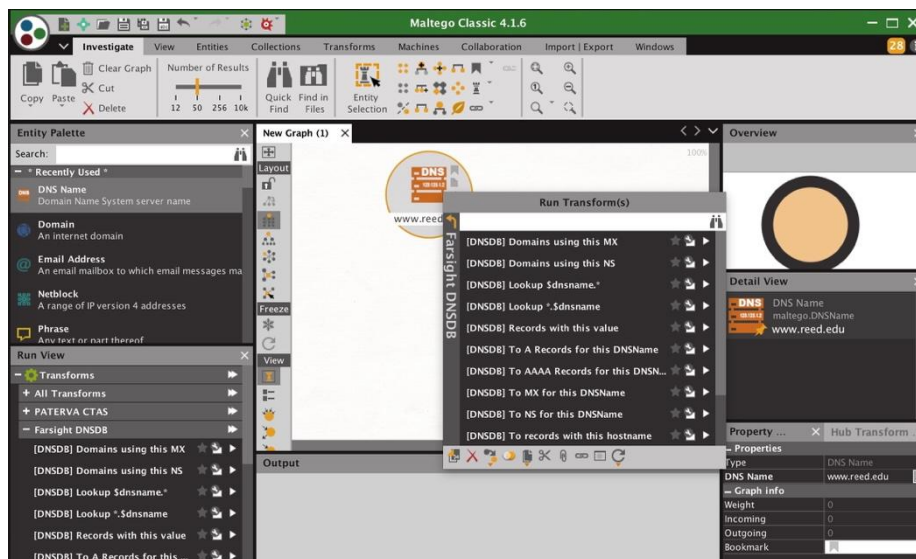
(3) The default name that's displayed (alpine.paterva.com) is NOT the name we're interested in, so double click on it and type in a different name. For this example, let's put in www.reed.edu After typing in that DNS Name, hit return. The result should look like Figure 11.

Figure 11. DNS Name Entity Now Showing The Name of Interest



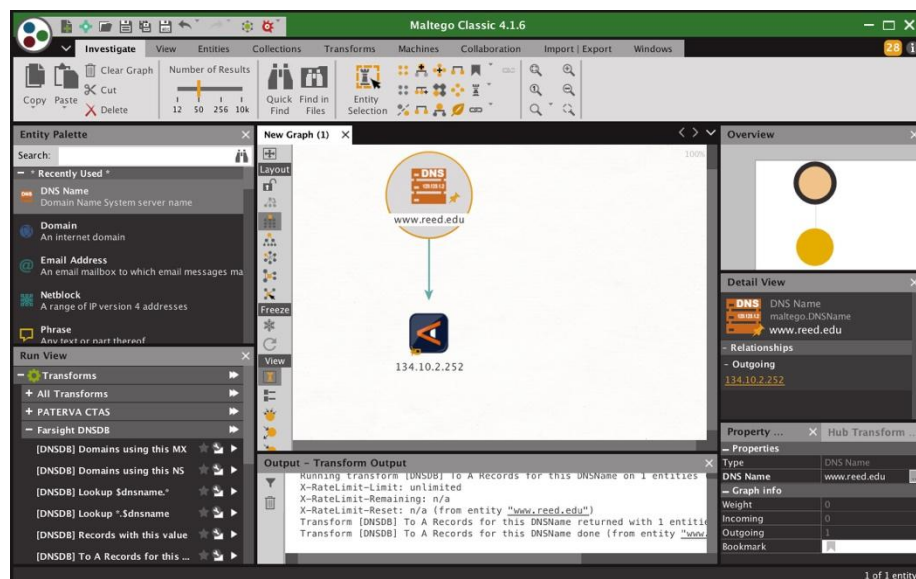
(4) Now need to decide which Transform we want to run on that Entity. Hold down the Control key and click on the Entity to see what transforms are available for the sort of Entity we're using. See Figure 12.

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



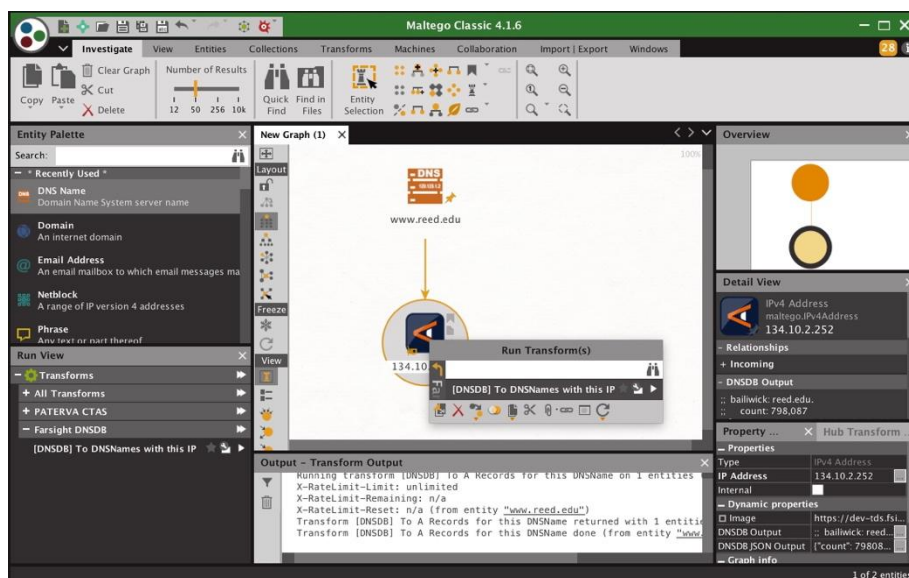
Note: Many different output formats are available, see the "View" menu to the left of the graph. If you prefer tables to diagrams, in particular, be sure to check out the tabular view

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.

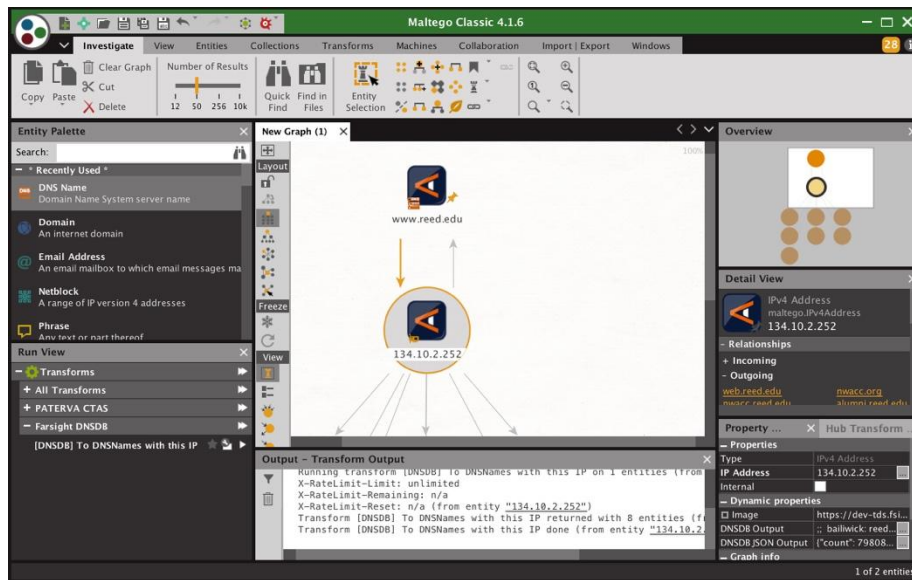
(5) We can now "chain" from our initial results to see what DNSNames (if any) also share that IP. In this case, the only Transform available to us is "To DNSNames with this IP" which makes our choice of Transform rather straightforward. See Figure 14.

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.

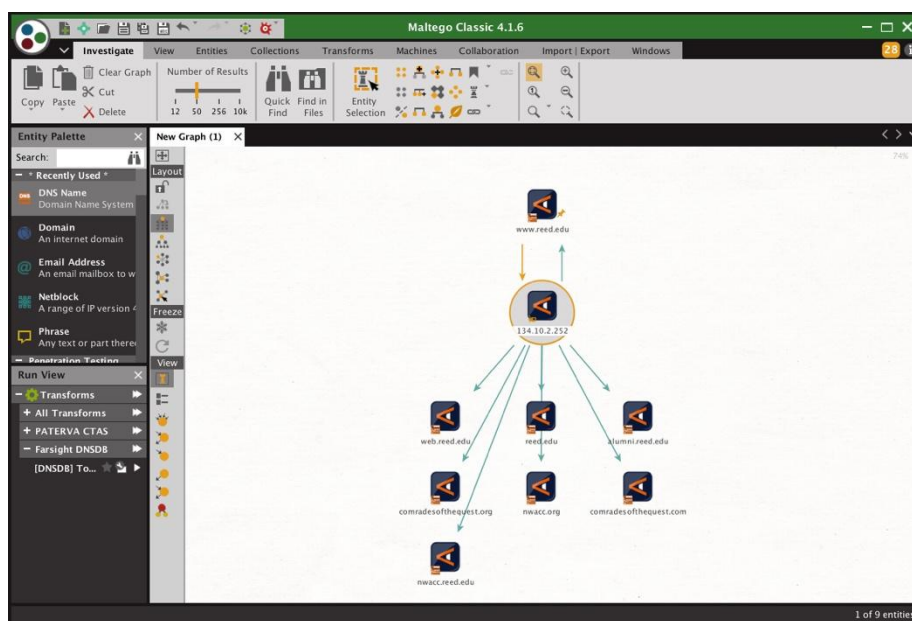
Figure 15. Results From Running The "To DNSNames with this IP" Transform



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

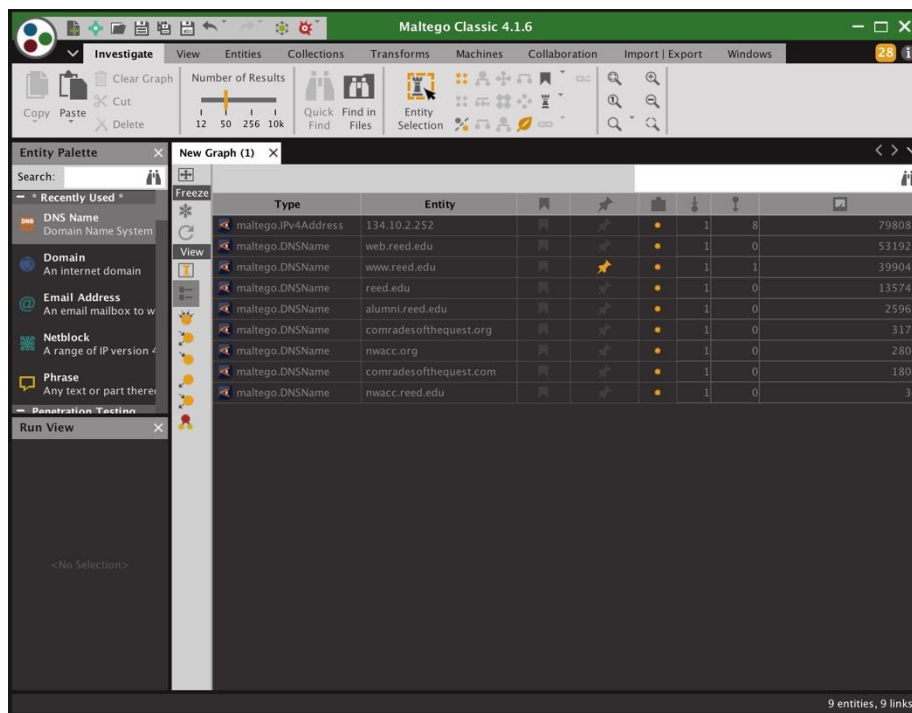
We'll close some of the panels we don't currently need, resize the "New Graph" window, and click on the magnifying glass at the top of the screen to "zoom to fit" the output. See Figure 16.

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 18, below.

- 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.

Figure 18. Sample Exported Graph

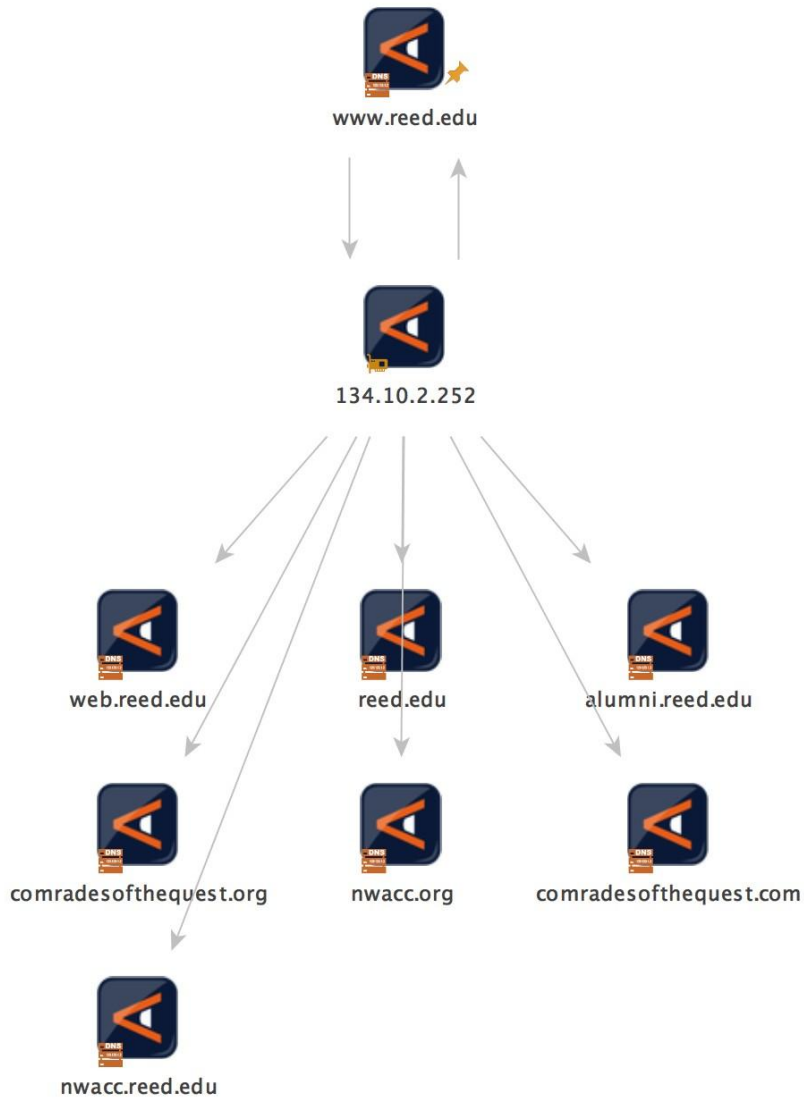


Figure 19. Sample Exported-as-CSV Table Data

```

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
  
```

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

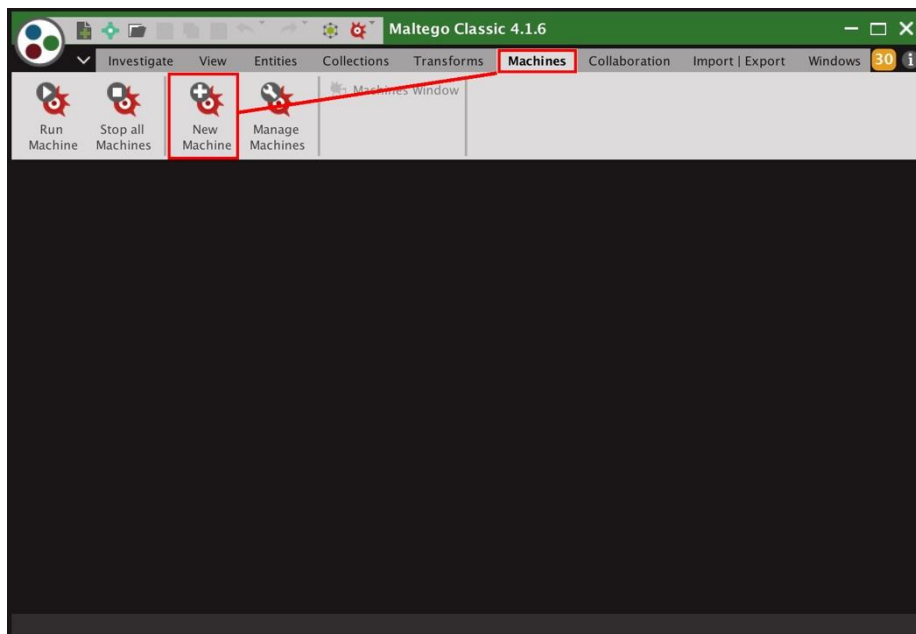
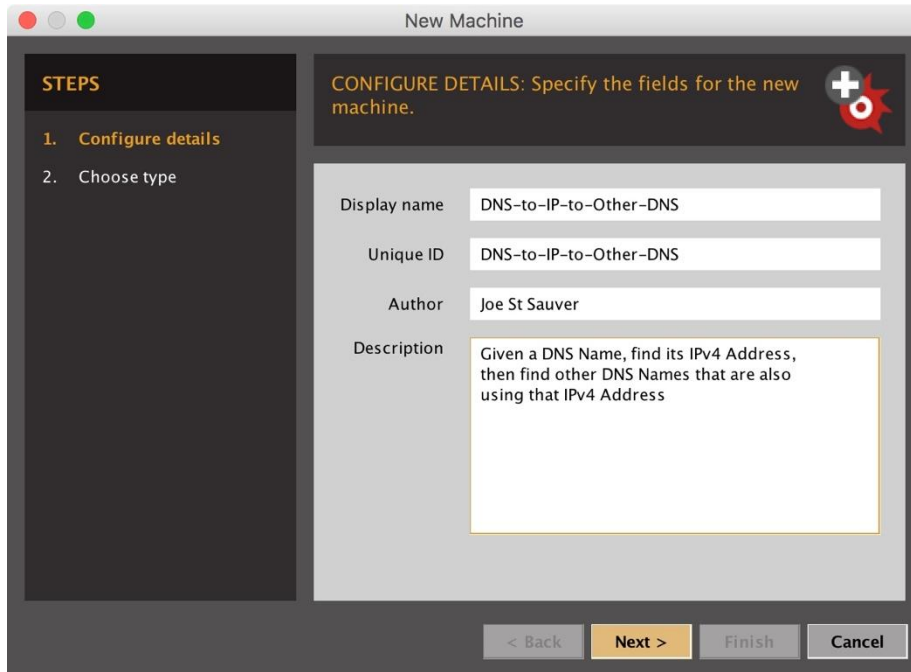
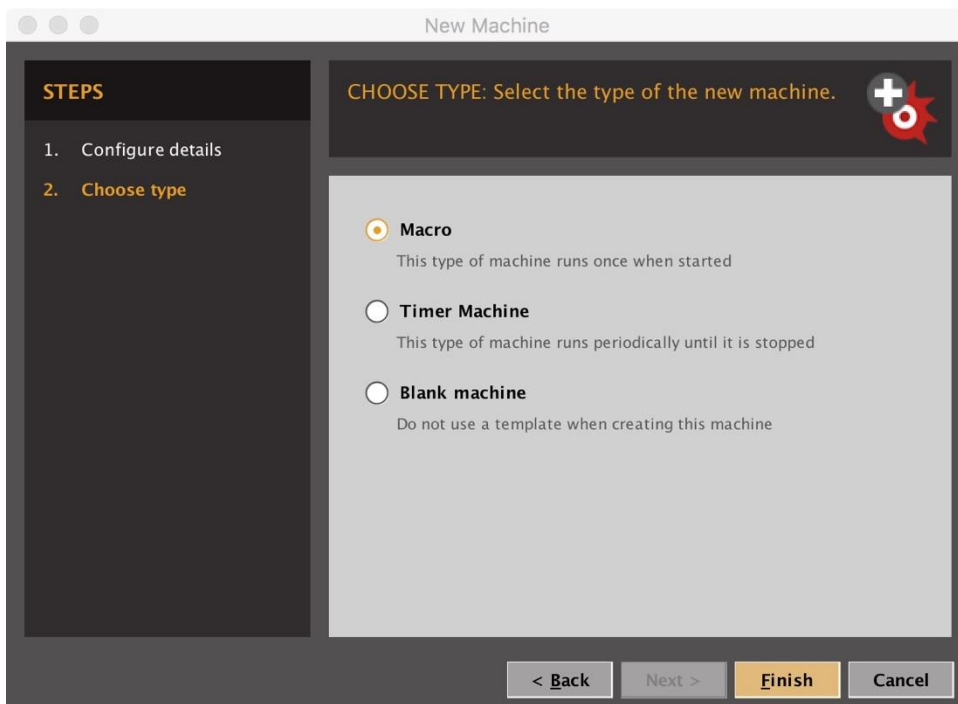


Figure 21. Supply configuration details



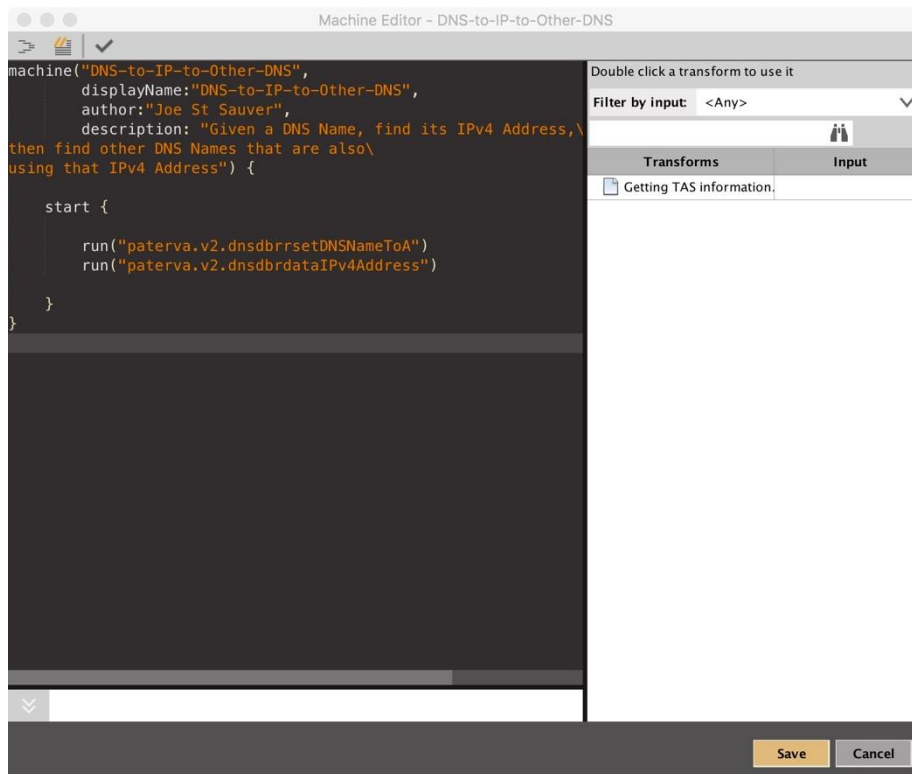
Complete the initial Machine by choosing it's type, as shown in Figure 22:

Figure 22. Choose the Type of Machine



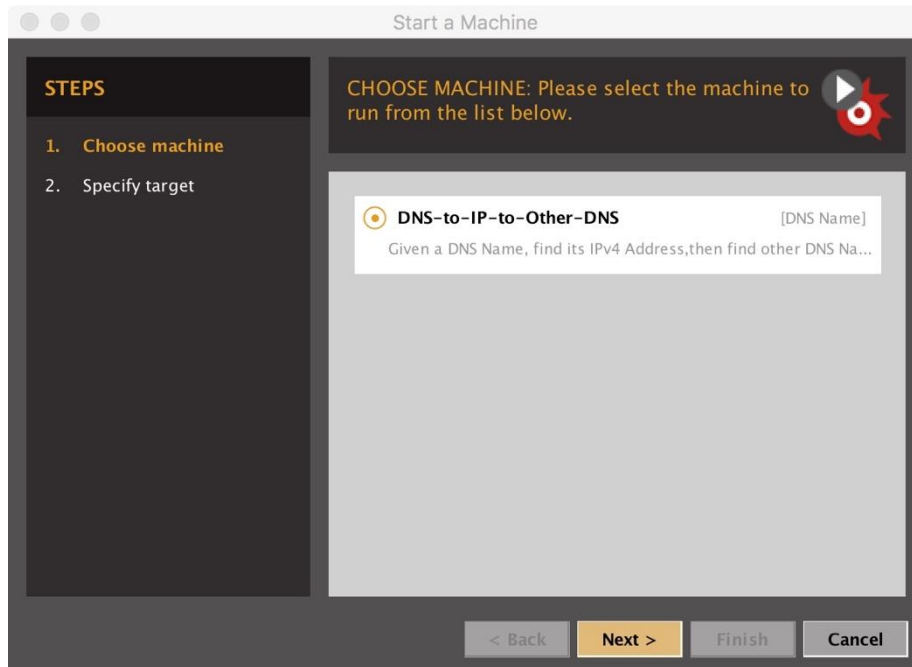
(2) You're now ready to customize the skeletal Machine outline you'll be given. We'll end up with what's shown in Figure 23.

Figure 23. Our Sample Machine's Simple Code



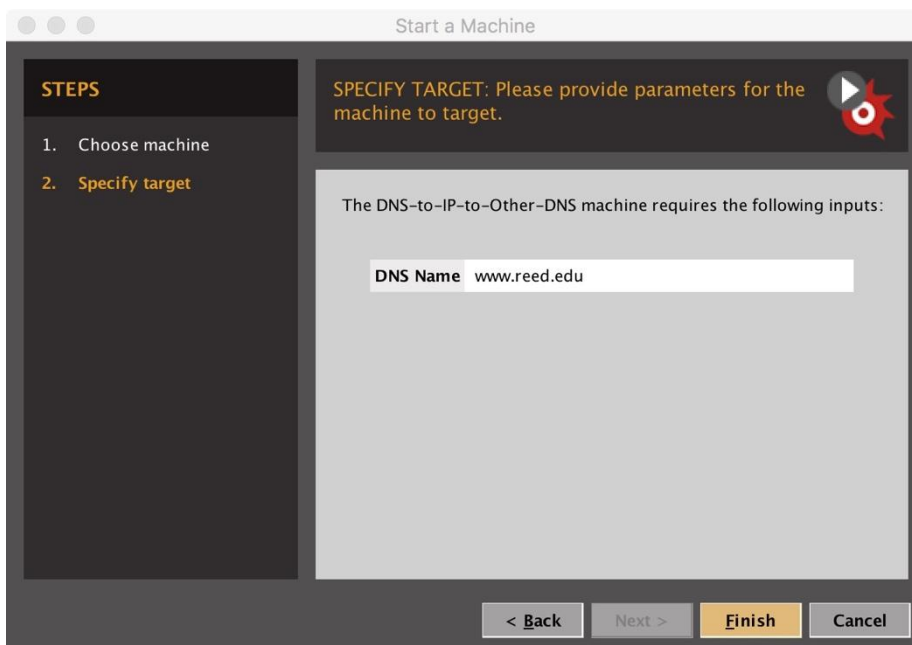
(3) After saving our machine, we can then run it. See Figure 24.

Figure 24. Picking the Machine We Want to Start



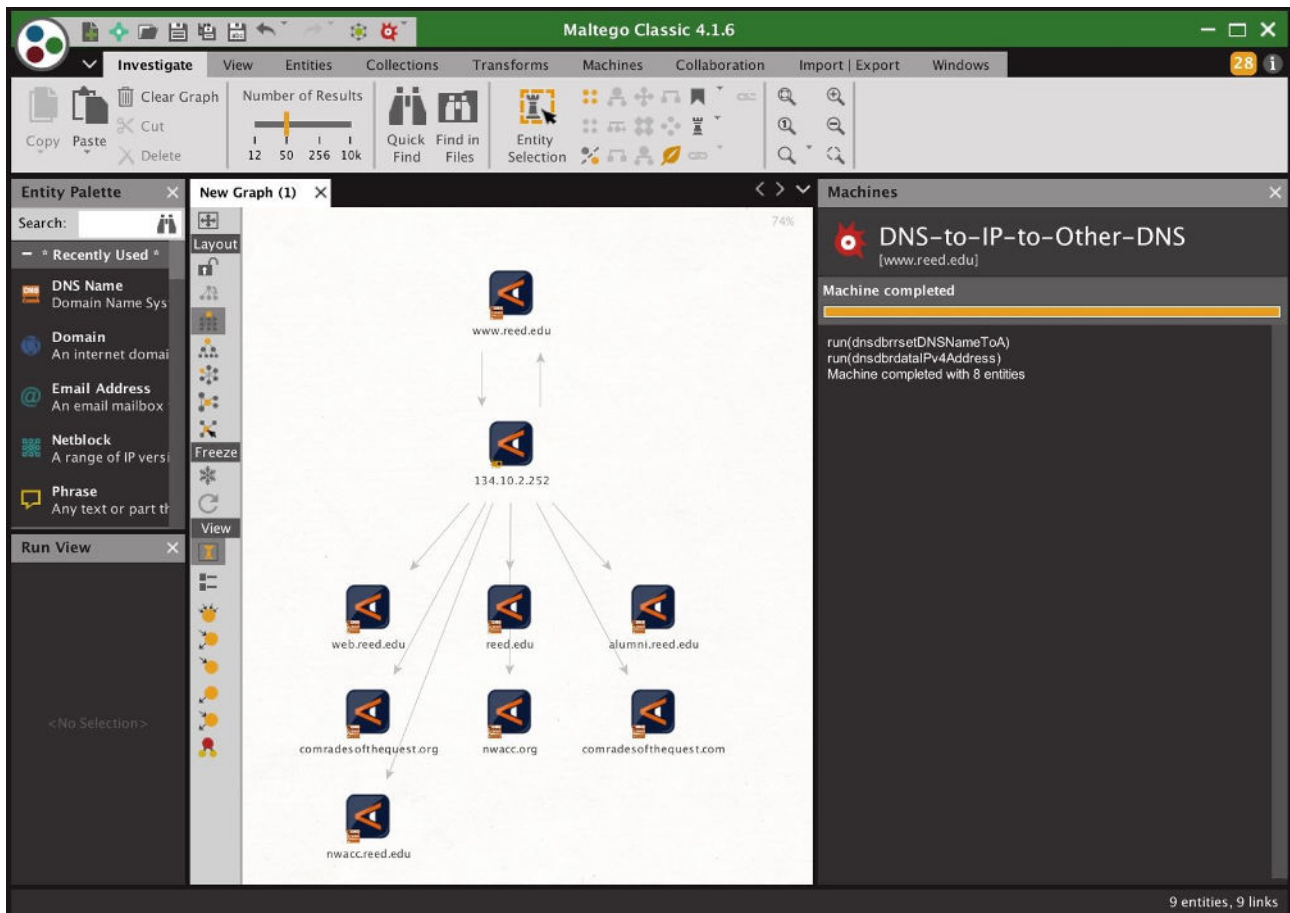
We also need to provide the name we want to run the Machine on... as a test, let's do www.reed.edu again.

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.

Figure 26. Machine's Output



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.

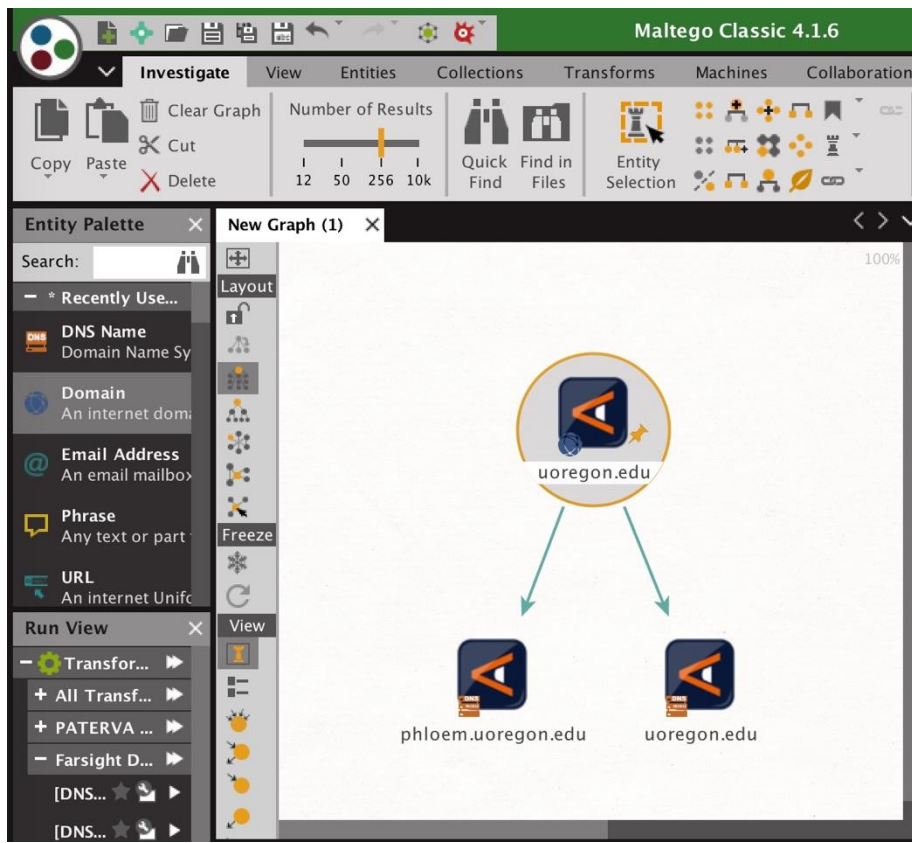
A Subtle But **Critically Important** "Side Effect" of The "Number-of-Results" Slider...

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:

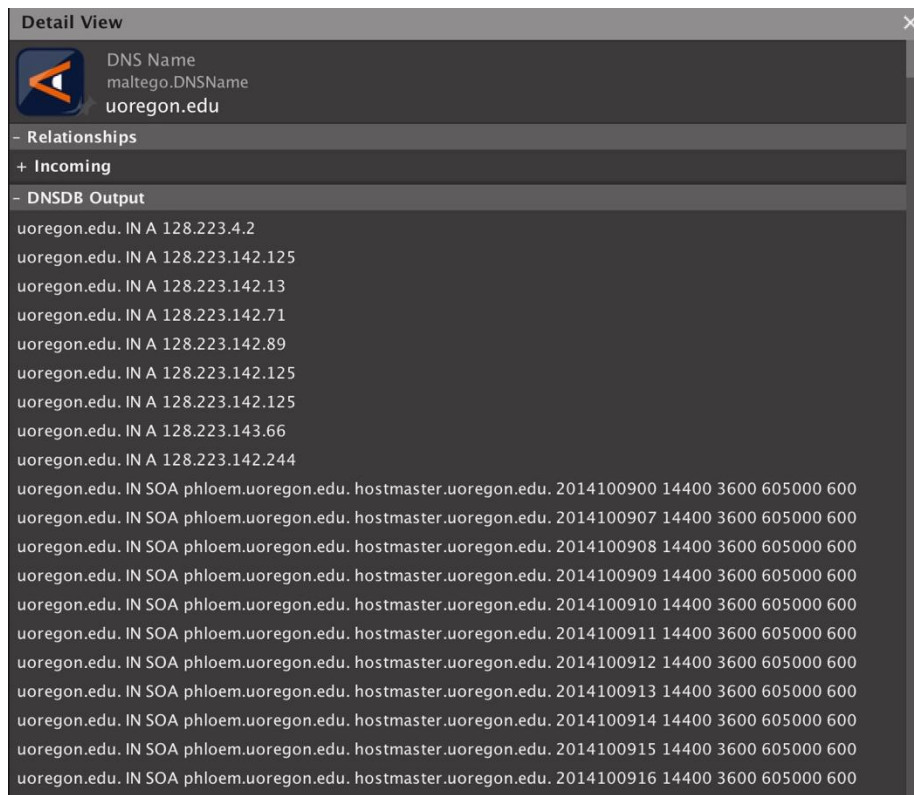
Figure 6: "Lookup *.\$Domain" Output With Number-of-Results Set to 256



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"

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

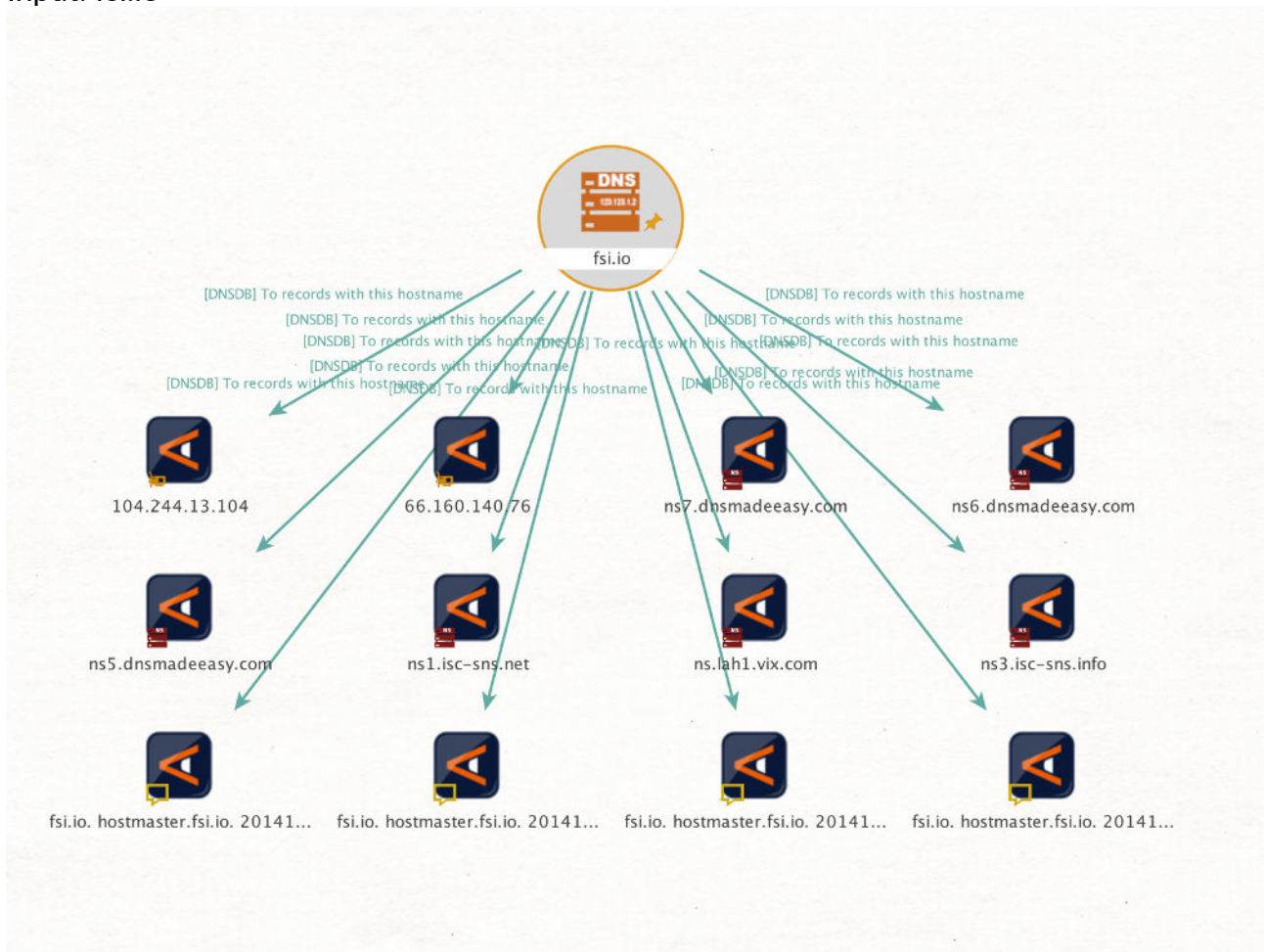
Note: The numbering of the Transforms in this appendix correspond to the numbers from Figure 8.

1. "To records with this hostname"

Name: paterva.v2.dnsdbrrsetDomain

Input Type: Domain

Input: fsi.io



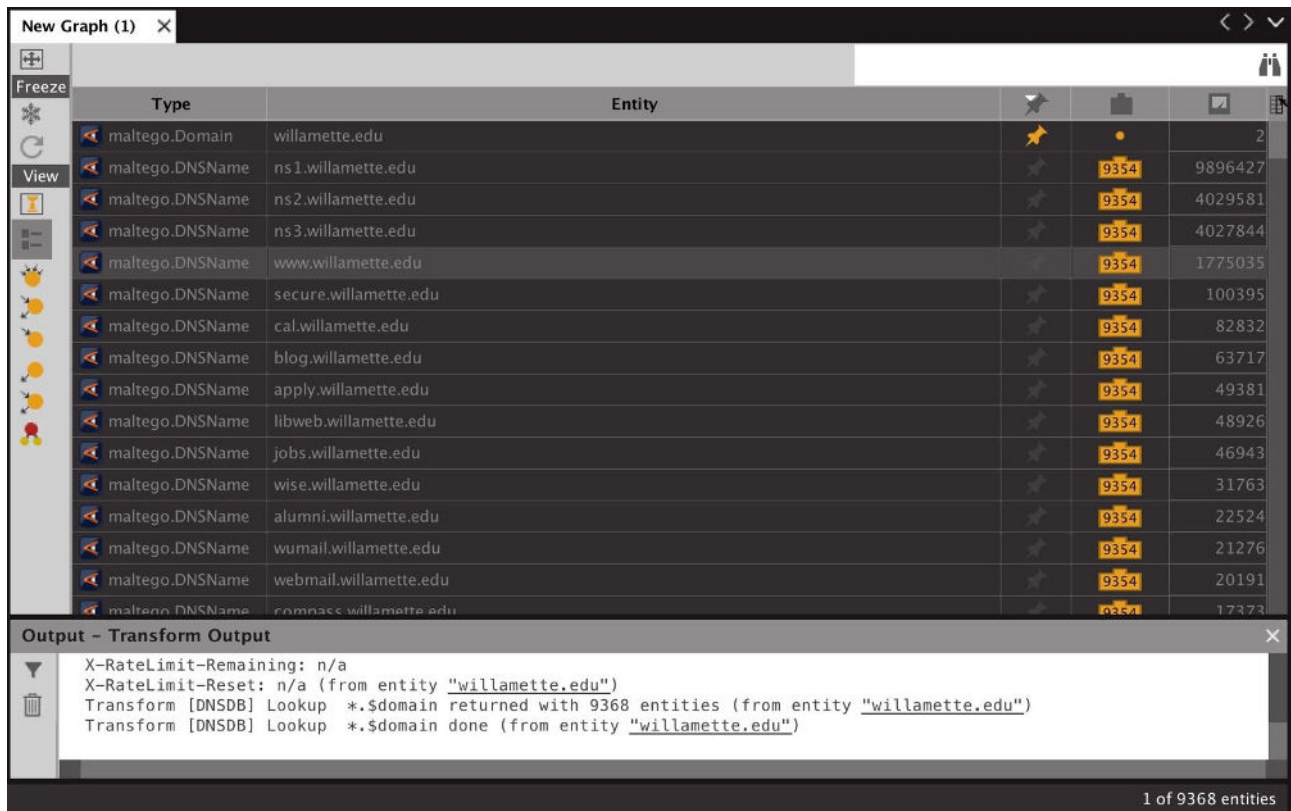
2. "Lookup *.\$domain"

Name: paterva.v2.dnsdbrrsetwclDomain

Input Type: Domain

Input: willamette.edu

Only selected columns shown



The screenshot displays the Maltego interface with a graph titled "New Graph (1)". The graph shows a central entity "willamette.edu" of type "maltego.Domain". From this entity, a transform has generated 9368 entities of type "maltego.DNSName". The visible entities in the graph are:

Type	Entity	Score	Count
maltego.Domain	willamette.edu		2
maltego.DNSName	ns1.willamette.edu	9354	9896427
maltego.DNSName	ns2.willamette.edu	9354	4029581
maltego.DNSName	ns3.willamette.edu	9354	4027844
maltego.DNSName	www.willamette.edu	9354	1775035
maltego.DNSName	secure.willamette.edu	9354	100395
maltego.DNSName	cal.willamette.edu	9354	82832
maltego.DNSName	blog.willamette.edu	9354	63717
maltego.DNSName	apply.willamette.edu	9354	49381
maltego.DNSName	libweb.willamette.edu	9354	48926
maltego.DNSName	jobs.willamette.edu	9354	46943
maltego.DNSName	wise.willamette.edu	9354	31763
maltego.DNSName	alumni.willamette.edu	9354	22524
maltego.DNSName	wumail.willamette.edu	9354	21276
maltego.DNSName	webmail.willamette.edu	9354	20191
maltego.DNSName	rompac.willamette.edu	9354	17373

The "Output - Transform Output" window shows the following text:

```
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "willamette.edu")
Transform [DNSDB] Lookup *.$domain returned with 9368 entities (from entity "willamette.edu")
Transform [DNSDB] Lookup *.$domain done (from entity "willamette.edu")
```

1 of 9368 entities

3. "Lookup *.\$domain/A"

Name: paterva.v2.dnsdbrrsetwclDomainA

Input Type: Domain

Input: willamette.edu

Only selected columns shown

The screenshot displays the Maltego interface with a graph of entities and a detail view for a specific entity.

Graph Data:

Type	Entity	9304	9900366
maltego.Domain	willamette.edu		0
maltego.DNSName	ns1.willamette.edu	9304	9900366
maltego.DNSName	ns2.willamette.edu	9304	4030952
maltego.DNSName	ns3.willamette.edu	9304	4029414
maltego.DNSName	www.willamette.edu	9304	1775150
maltego.DNSName	willamette.edu	9304	491763
maltego.DNSName	secure.willamette.edu	9304	100451
maltego.DNSName	cal.willamette.edu	9304	82884
maltego.DNSName	library.willamette.edu	9304	82749
maltego.DNSName	blog.willamette.edu	9304	63728
maltego.DNSName	libweb.willamette.edu	9304	48926
maltego.DNSName	wise.willamette.edu	9304	31779
maltego.DNSName	smtp1.willamette.edu	9304	30460
maltego.DNSName	smtp2.willamette.edu	9304	30454
maltego.DNSName	smtp3.willamette.edu	9304	28246
maltego.DNSName	webmail.willamette.edu	9304	20191
maltego.DNSName	mail.willamette.edu	9304	16327
maltego.DNSName	ldap.willamette.edu	9304	16096

Detail View for library.willamette.edu:

- DNS Name:** maltego.DNSName, library.willamette.edu
- Relationships:** + Incoming
- DNSDB Output:** library.willamette.edu. IN A 158.104.100.73
- DNSDB JSON Output:** {"count": 82749, "time_first": 1339457035, "rrtype": "A", "rrname": "library.willamette.edu.", "bailiwick": "willamette.edu.", "rdata": "158.104.100.73", "time_last": 1521288550}
- Generator detail:**
 - Source:** willamette.edu (Domain)
 - Transform:** [DNSDB] Lookup *.\$domain/A
 - Gen. date:** 2018-03-17 14:49:35.174 -0700

Output - Transform Output: (Empty)

1 of 9305 entities

4. "Lookup *.\$domain/AAAA"

Name: paterva.v2.dnsdbrrsetwclDomainAAAA

Input Type: Domain

Input: uoregon.edu

Only selected columns shown

The screenshot shows the Maltego interface with a graph of entities and a detail view for 'phloem.uoregon.edu'. The graph table lists various DNSName entities for the domain uoregon.edu, each with a count of 228. The detail view shows relationships, incoming connections, and DNSDB output for the selected entity.

Type	Entity	Count
maltego.Domain	uoregon.edu	0
maltego.DNSName	phloem.uoregon.edu	228
maltego.DNSName	ruminant.uoregon.edu	228
maltego.DNSName	dns.cs.uoregon.edu	228
maltego.DNSName	ds1.cs.uoregon.edu	228
maltego.DNSName	ds2.cs.uoregon.edu	228
maltego.DNSName	wc-www.uoregon.edu	228
maltego.DNSName	mirror.uoregon.edu	228
maltego.DNSName	uowc-www.uoregon.edu	228
maltego.DNSName	it-prod.uoregon.edu	228
maltego.DNSName	webmail.uoregon.edu	228
maltego.DNSName	uoregon.edu	228
maltego.DNSName	ad-cc-dc1.ad.uoregon.edu	228
maltego.DNSName	network-services.uoregon.edu	228
maltego.DNSName	mail.cs.uoregon.edu	228
maltego.DNSName	mx2.uoregon.edu	228
maltego.DNSName	mx1.uoregon.edu	228

Output - Transform Output

```
Running transform [DNSDB] Lookup *.$domain/AAAA on 1 entities (from entity "uoregon.edu")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon.edu")
Transform [DNSDB] Lookup *.$domain/AAAA returned with 228 entities (from entity "uoregon.edu")
Transform [DNSDB] Lookup *.$domain/AAAA done (from entity "uoregon.edu")
```

Detail View

DNS Name
maltego.DNSName
phloem.uoregon.edu

Relationships

+ Incoming

- DNSDB Output

```
phloem.uoregon.edu. IN AAAA 2001:468:d01:20::80df:203
phloem.uoregon.edu. IN AAAA 2001:468:d01:20::80df:203
phloem.uoregon.edu. IN AAAA 2001:468:d01:20::80df:203
phloem.uoregon.edu. IN AAAA 2001:468:d01:20::80df:203
phloem.uoregon.edu. IN AAAA 2001:468:d01:20::80df:203
phloem.uoregon.edu. IN AAAA 2001:468:d01:20::80df:203
```

- DNSDB JSON Output

```
{"count": 2882, "rrtype": "AAAA", "rrname": "phloem.uoregon.edu.", "zone_time_first": 1271183957, "zone_time_last": 1521316806, "bailiwick": ".", "rdata": "2001:468:d01:20::80df:2023"}
{"count": 149302168, "time_first": 1277348940, "rrtype": "AAAA", "rrname": "phloem.uoregon.edu.", "bailiwick": ".", "rdata": "2001:468:d01:20::80df:2023", "time_last": 1521324247}
{"count": 4, "time_first": 1515995036, "rrtype": "AAAA", "rrname": "phloem.uoregon.edu.", "bailiwick": "edu.", "rdata": "2001:468:d01:20::80df:2023", "time_last": 1516337018}
{"count": 2, "time_first": 1515816181, "rrtype": "AAAA", "rrname": "phloem.uoregon.edu.", "bailiwick": "edu.", "rdata": "2001:468:d01:20::80df:2003", "time_last": 1515816181}
{"count": 82688627, "time_first": 1277348895, "rrtype": "AAAA", "rrname": "phloem.uoregon.edu.", "bailiwick": "edu.", "rdata": "2001:468:d01:20::80df:2023", "time_last": 1521323537}
```

1 of 229 entities

5. "Lookup *.\$domain/CNAME"

Name: paterva.v2.dnsdbrrsetwclDomainCNAME

Input Type: Domain

Input: uoregon.edu

Only selected columns shown

The screenshot displays the Maltego interface with a graph of DNS records and a detail view for a specific record.

Graph Data:

Type	Entity	Count	Score
maltego.Domain	uoregon.edu	0	
maltego.DNSName	www.uoregon.edu	6704	1241127
maltego.DNSName	admissions.uoregon.edu	6704	648052
maltego.DNSName	around.uoregon.edu	6704	479969
maltego.DNSName	giving.uoregon.edu	6704	363769
maltego.DNSName	financialaid.uoregon.edu	6704	329545
maltego.DNSName	sync.uoregon.edu	6704	314860
maltego.DNSName	mirror.nic.uoregon.edu	6704	286122
maltego.DNSName	gradschool.uoregon.edu	6704	235136
maltego.DNSName	visit.uoregon.edu	6704	225040
maltego.DNSName	housing.uoregon.edu	6704	216042
maltego.DNSName	business.uoregon.edu	6704	190870
maltego.DNSName	mappinghistory.uoregon.edu	6704	186682
maltego.DNSName	uonews.uoregon.edu	6704	170560
maltego.DNSName	registrar.uoregon.edu	6704	166690
maltego.DNSName	uocatalog.uoregon.edu	6704	145871
maltego.DNSName	tep.uoregon.edu	6704	142330

Detail View:

DNS Name
maltego.DNSName
admissions.uoregon.edu

Relationships

+ Incoming

- DNSDB Output
admissions.uoregon.edu. IN CNAME secureserver.uoregon.edu
admissions.uoregon.edu. IN CNAME drupal-cluster3.uoregon.edu

- DNSDB JSON Output

```
{
  "count": 136558,
  "time_first": 1277542603,
  "rrtype": "CNAME",
  "rrname": "admissions.uoregon.edu",
  "bailiwick": "uoregon.edu",
  "rdata": "secureserver.uoregon.edu",
  "time_last": 1414097890
}
```

```
{
  "count": 648052,
  "time_first": 1412801439,
  "rrtype": "CNAME",
  "rrname": "admissions.uoregon.edu",
  "bailiwick": "uoregon.edu",
  "rdata": "drupal-cluster3.uoregon.edu",
  "time_last": 1521319260
}
```

- Generator detail

Source	uoregon.edu	(Domain)
Transform	[DNSDB] Lookup *.\$domain/CNAME	
Gen. date	2018-03-17 15:29:46.955 -0700	

Output - Transform Output

```
Running transform [DNSDB] Lookup *.$domain/CNAME on 1 entities (from entity "uoregon.edu")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon.edu")
Transform [DNSDB] Lookup *.$domain/CNAME returned with 6704 entities (from entity "uoregon.edu")
Transform [DNSDB] Lookup *.$domain/CNAME done (from entity "uoregon.edu")
```

1 of 6705 entities

6. "Lookup \$domain.*"

Name: paterva.v2.dnsdbrrsetwcrDomain

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*.

Type	Entity	Value
maltego.DNSName	uoregon.us5.list-managez.com	787
maltego.DNSName	uoregon.dc4.pageuppeople.com	787
maltego.DNSName	uoregon.scalefunder.com	787
maltego.Domain	uoregon.net	53
maltego.DNSName	uoregon.ebib.com.libproxy.uoregon.edu	787
maltego.DNSName	uoregon.maps.arcgis.com	787
maltego.DNSName	uoregon.simnetonline.com	787
maltego.DNSName	uoregon.us14.list-manage.com	787
maltego.DNSName	uoregon.chiomega.com	787
maltego.Domain	uoregon.us	53
maltego.DNSName	uoregon.us1.list-manage.com	787
maltego.DNSName	uoregon.wix.com	787
maltego.DNSName	uoregon.us12.list-manage1.com	787
maltego.DNSName	uoregon.kanopystreaming.com	787
maltego.DNSName	uoregon.transfer.org	787
maltego.DNSName	uoregon.us11.list-manage.com	787

```

Output - Transform Output
Running transform [DNSDB] Lookup $domain.* on 1 entities (from entity "uoregon")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $domain.* returned with 840 entities (from entity "uoregon")
Transform [DNSDB] Lookup $domain.* done (from entity "uoregon")
    
```

Detail View

Domain
maltego.Domain
uoregon.net

+ Incoming

- DNSDB Output

uoregon.net. IN NS ns1.sprserver.com.
uoregon.net. IN NS ns2.sprserver.com.
uoregon.net. IN NS ns1.sedoparking.com.
uoregon.net. IN NS ns2.sedoparking.com.
uoregon.net. IN NS ns63.domaincontrol.com.
uoregon.net. IN NS ns64.domaincontrol.com.
uoregon.net. IN NS ns1.sprserver.com.
uoregon.net. IN NS ns2.sprserver.com.
uoregon.net. IN NS ns1.sedoparking.com.
uoregon.net. IN NS ns2.sedoparking.com.
uoregon.net. IN NS ns63.domaincontrol.com.
uoregon.net. IN NS ns64.domaincontrol.com.
uoregon.net. IN NS ns1.sedoparking.com.
uoregon.net. IN NS ns2.sedoparking.com.
uoregon.net. IN NS ns63.domaincontrol.com.
uoregon.net. IN NS ns64.domaincontrol.com.
uoregon.net. IN NS ns1.sedoparking.com.
uoregon.net. IN NS ns2.sedoparking.com.
uoregon.net. IN NS ns63.domaincontrol.com.
uoregon.net. IN NS ns64.domaincontrol.com.
uoregon.net. IN MX 0 localhost.
uoregon.net. IN MX 0 mail.nickstel.com.
uoregon.net. IN MX smtp.secureserver.net.
uoregon.net. IN MX 10 mailstore1.secureserver.net.

1 of 841 entities

7. "Lookup \$domain.* /A"

Name: paterva.v2.dnsdbrrsetwcrDomainA

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.

The screenshot displays the Maltego interface with a graph and a detail view. The graph shows a table of entities:

Type	Entity	Count	Score
maltego.Domain	uoregon	0	
maltego.DNSName	uoregon.edu	432	2114581
maltego.DNSName	uoregon.studentaidcalculator.com	432	54906
maltego.DNSName	uoregon.orgsync.com	432	14220
maltego.DNSName	uoregon.medicatconnect.com	432	8843
maltego.DNSName	uoregon.academicworks.com	432	7765
maltego.DNSName	uoregon.collegescheduler.com	432	7668
maltego.DNSName	uoregon.interactyx.com	432	7236
maltego.DNSName	uoregon.imodules.com	432	6939
maltego.DNSName	uoregon.spoonuniversity.com	432	5724
maltego.DNSName	uoregon.myonlinecamp.com	432	1376
maltego.DNSName	uoregon.sidearmsports.com	432	1365
maltego.DNSName	uoregon.libapps.com	432	1207
maltego.DNSName	uoregon.kappdelta.org	432	1149
maltego.DNSName	uoregon.edu.education2020.us	432	1106
maltego.DNSName	uoregon.technologypublisher.com	432	1103

The detail view for 'uoregon.kappdelta.org' shows the following information:

- DNS Name:** maltego.DNSName, uoregon.kappdelta.org
- Relationships:** + Incoming
- DNSDB Output:** uoregon.kappdelta.org. IN A 54.81.65.83, uoregon.kappdelta.org. IN A 209.208.116.50
- DNSDB JSON Output:** [{"count": 2832, "time_first": 1418943701, "rrtype": "A", "rrname": "uoregon.kappdelta.org.", "balliwick": "kappdelta.org.", "rdata": "54.81.65.83", "time_last": 1521146271}, {"count": 1149, "time_first": 1334251236, "rrtype": "A", "rrname": "uoregon.kappdelta.org.", "balliwick": "kappdelta.org.", "rdata": "209.208.116.50", "time_last": 1372852174}]
- Generator detail:** Source: uoregon (Domain), Transform: [DNSDB] Lookup \$domain.* /A, Gen. date: 2018-03-17 15:51:16.879 -0700

The output window shows the following text:

```
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $domain.* /A returned with 432 entities (from entity "uoregon")
Transform [DNSDB] Lookup $domain.* /A done (from entity "uoregon")
```

1 of 433 entities

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.

The screenshot displays the Maltego interface. The main graph shows a central node 'uoregon' with arrows pointing to several other nodes: 'uoregon.edu', 'uoregon.mycampusdirector2.com', 'uoregon.callistocampus.org', 'uoregon.wtf', 'uoregon.cbinsights.com', 'uoregon.moneybird.com', and 'uoregon.api.mal.blindsidenetwor...'. The 'uoregon.co' node is highlighted with a yellow circle. The 'Detail View' panel on the right shows the following information:

- DNS Name:** maltego.DNSName, uoregon.co
- Relationships:** + Incoming
- DNSDB Output:**
 - uoregon.co. IN AAAA 2400.cb00:2048:1::681f:42e0
 - uoregon.co. IN AAAA 2400.cb00:2048:1::681f:43e0
- DNSDB JSON Output:**

```
[{"count": 11, "time_first": 1497608815, "rrtype": "AAAA", "rrname": "uoregon.co.", "balliwick": "uoregon.co.", "rdata": "2400.cb00:2048:1::681f:42e0", "time_last": 1498034224}
{"count": 11, "time_first": 1497608815, "rrtype": "AAAA", "rrname": "uoregon.co.", "balliwick": "uoregon.co.", "rdata": "2400.cb00:2048:1::681f:43e0", "time_last": 1498034224}]
```
- Generator detail:**
 - Source: uoregon (Domain)
 - Transform: [DNSDB] Lookup \$domain.*/AAAA
 - Gen. date: 2018-03-17 15:54:44.213 -0700

The 'Output - Transform Output' panel at the bottom shows the following log messages:

```
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $domain.*/AAAA returned with 8 entities (from entity "uoregon")
Transform [DNSDB] Lookup $domain.*/AAAA done (from entity "uoregon")
```

1 of 9 entities

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.

The screenshot displays the Maltego interface with a transform output table and a detail view for a specific entity.

Transform Output Table:

Type	Entity	Count	Score
maltego.Domain	uoregon	0	166054
maltego.DNSName	uoregon.spoonuniversity.com	346	19600
maltego.DNSName	uoregon.sharepoint.com	346	11891
maltego.DNSName	uoregon.kappa.org	346	5932
maltego.DNSName	uoregon.collegescheduler.com	346	4004
maltego.DNSName	uoregon.mhcampus.com	346	3192
maltego.DNSName	uoregon.tridelta.org	346	1979
maltego.DNSName	uoregon.kappadelta.org	346	1876
maltego.DNSName	uoregon.imodules.com	346	1791
maltego.DNSName	uoregon.us2.list-manage.com	346	1158
maltego.DNSName	uoregon.us2.list-manage1.com	346	846
maltego.DNSName	uoregon.instructure.com	346	842
maltego.DNSName	uoregon.hosted.panopto.com	346	769
maltego.DNSName	uoregon.us2.list-manage2.com	346	677
maltego.DNSName	uoregon.libcal.com	346	651
maltego.DNSName	uoregon.myonlinetecamp.com	346	596
maltego.DNSName	uoregon.goldenkey.org	346	465
maltego.DNSName	uoregon.us1.list-manage1.com	346	

Detail View:

DNS Name
maltego.DNSName
uoregon.sharepoint.com

Relationships

+ Incoming

- DNSDB Output
uoregon.sharepoint.com. IN CNAME prodnet296-253a0000.sharepointonline.com
uoregon.sharepoint.com. IN CNAME prodnet296-253edgea0000.sharepointonline.com

- DNSDB JSON Output

```
{
  "count": 10811,
  "time_first": 1431563656,
  "rrtype": "CNAME",
  "rrname": "uoregon.sharepoint.com.",
  "bailiwick": "sharepoint.com.",
  "rdata": "prodnet296-253a0000.sharepointonline.com.akadns.net.",
  "time_last": 1486445206
}
```

```
{
  "count": 19600,
  "time_first": 1486254008,
  "rrtype": "CNAME",
  "rrname": "uoregon.sharepoint.com.",
  "bailiwick": "sharepoint.com.",
  "rdata": "prodnet296-253edgea0000.sharepointonline.com.akadns.net.",
  "time_last": 1521321045
}
```

Generator detail

Source: uoregon (Domain)
Transform: [DNSDB] Lookup \$domain.*/CNAME
Gen. date: 2018-03-17 15:59:32.433 -0700

Output - Transform Output

```
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $domain.*/CNAME returned with 346 entities (from entity "uoregon")
Transform [DNSDB] Lookup $domain.*/CNAME done (from entity "uoregon")
```

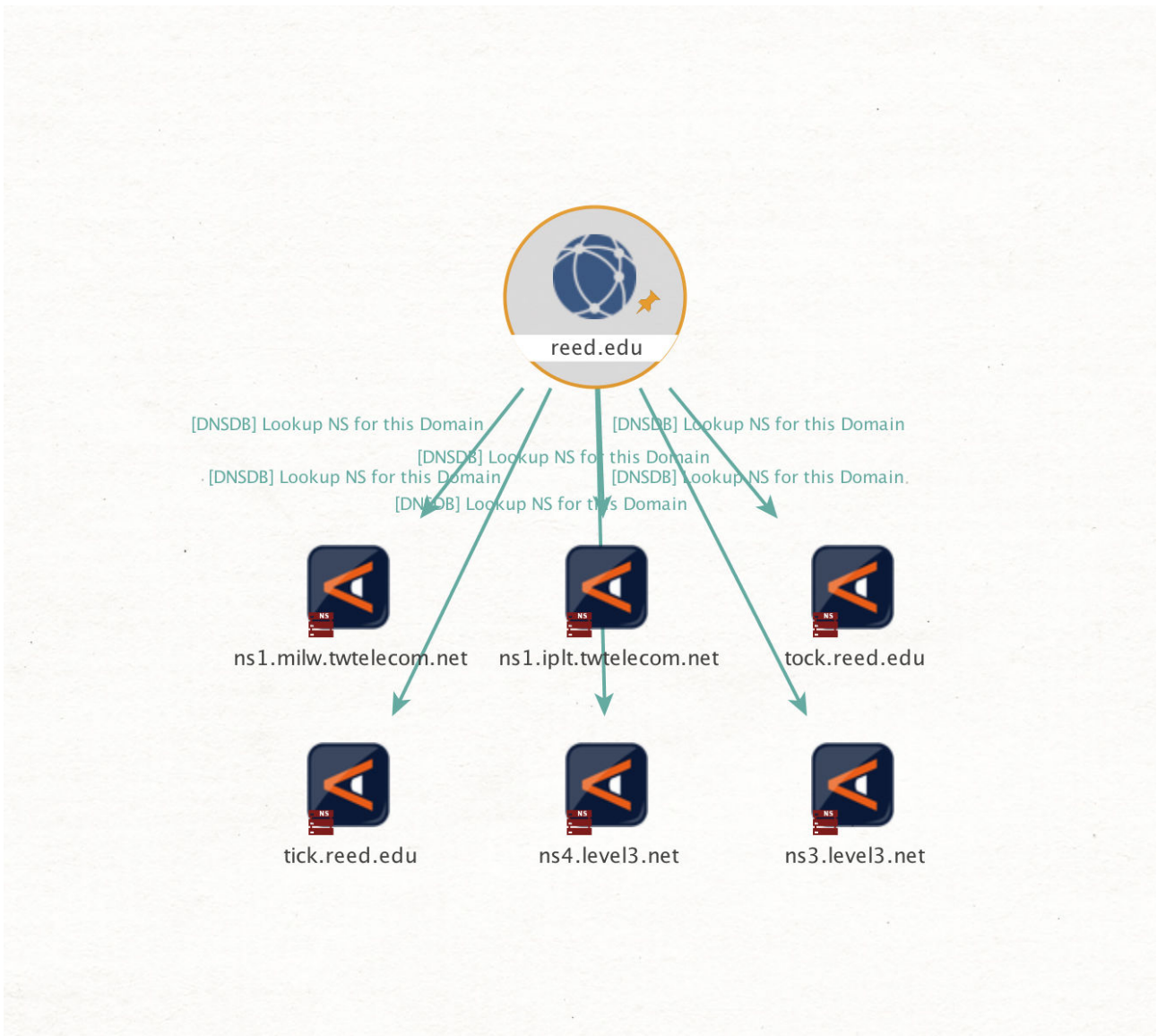
1 of 347 entities

10. "Lookup NS for this Domain"

Name: paterva.v2.dnsdbrrsetDomainNS

Input Type: Domain

Input: reed.edu

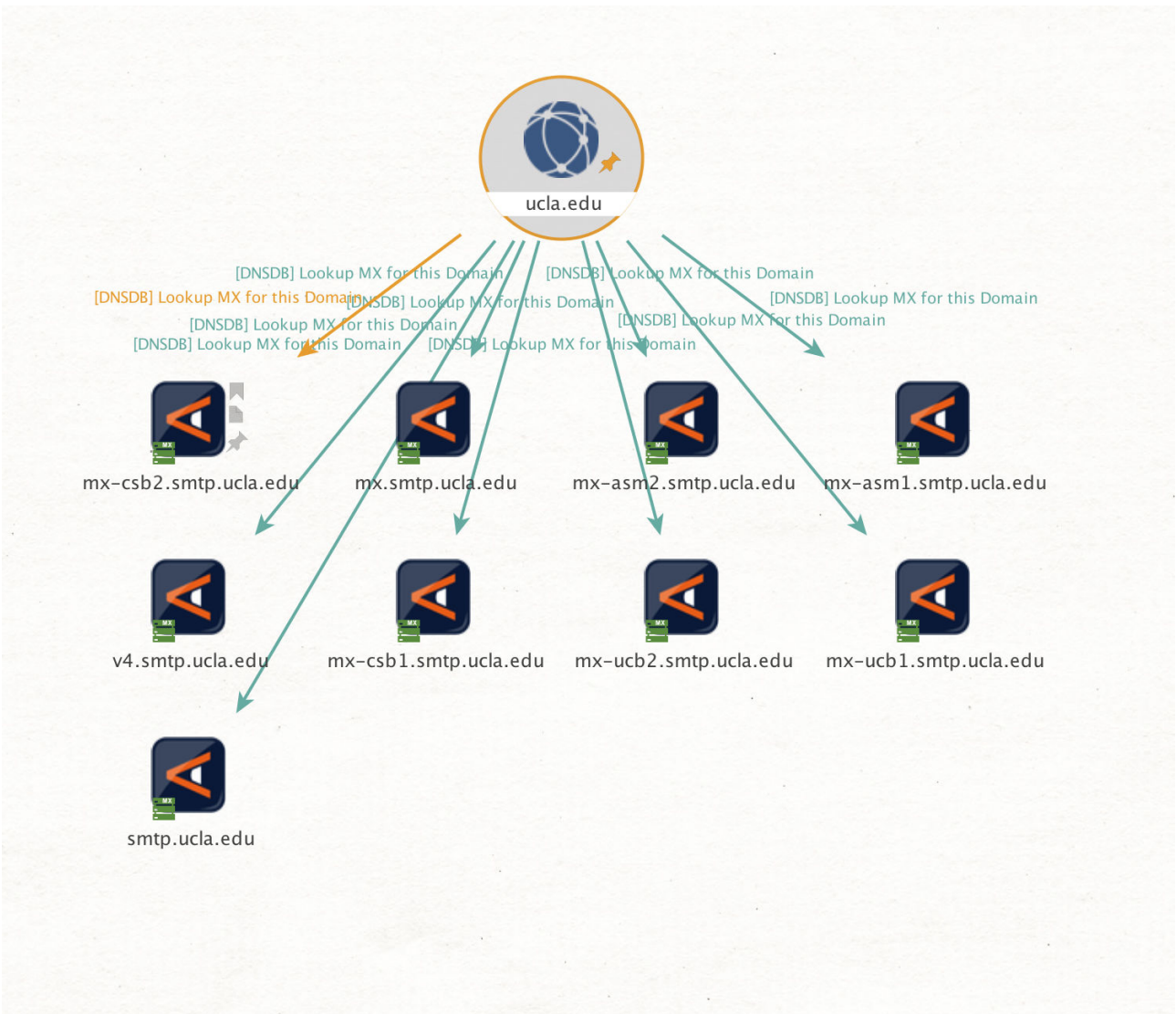


11. "Lookup MX for this Domain"

Name: paterva.v2.dnsdbrrsetDomainMX

Input Type: Domain

Input: ucla.edu

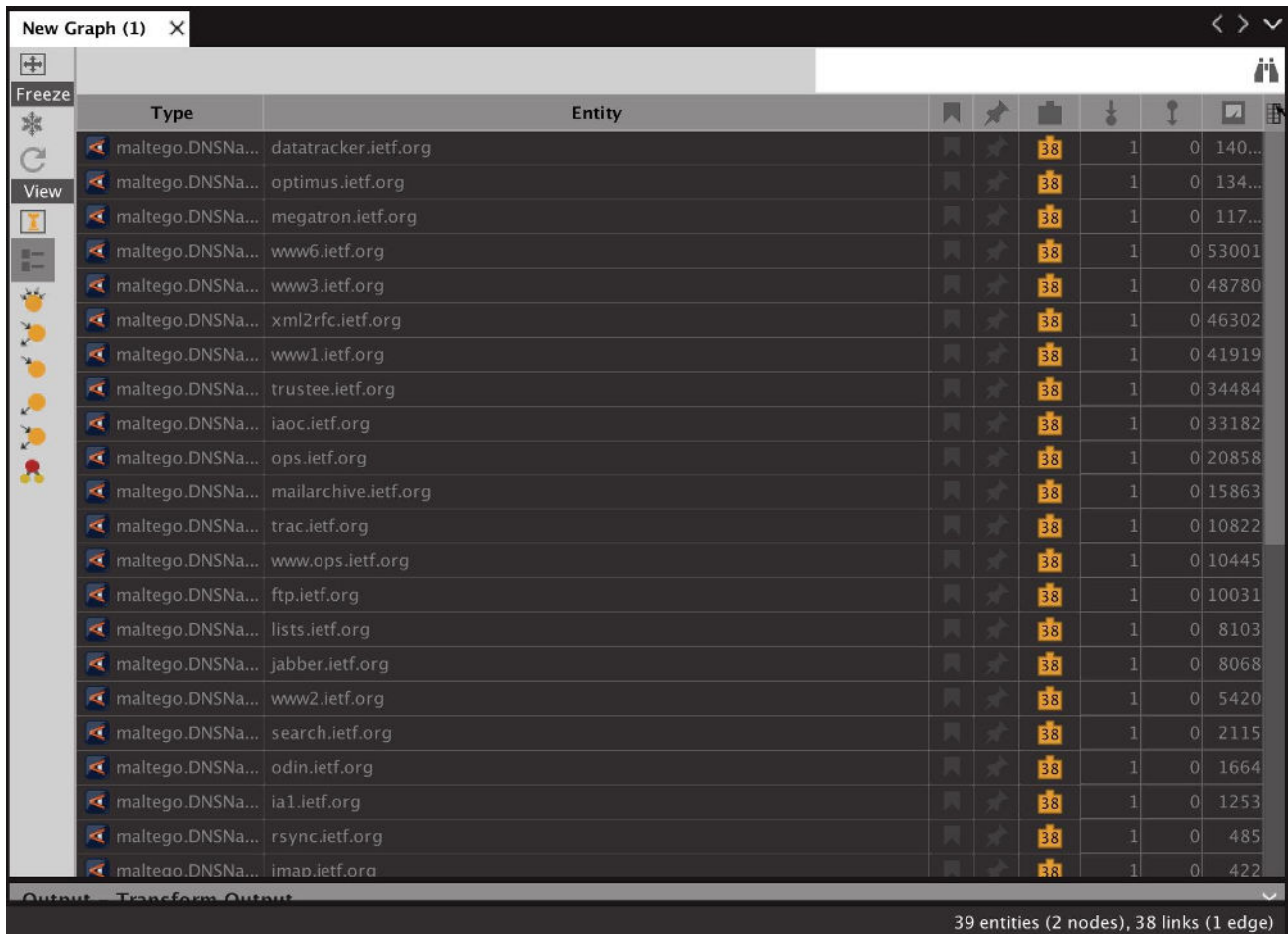


12. "To DNSNames with this value"

Name: paterva.v2.dnsdbdataDomain

Input Type: Domain

Input: ietf.org



New Graph (1) X

Type	Entity	38	1	0	140...
maltego.DNSNa...	datatracker.ietf.org	38	1	0	140...
maltego.DNSNa...	optimus.ietf.org	38	1	0	134...
maltego.DNSNa...	megatron.ietf.org	38	1	0	117...
maltego.DNSNa...	www6.ietf.org	38	1	0	53001
maltego.DNSNa...	www3.ietf.org	38	1	0	48780
maltego.DNSNa...	xml2rfc.ietf.org	38	1	0	46302
maltego.DNSNa...	www1.ietf.org	38	1	0	41919
maltego.DNSNa...	trustee.ietf.org	38	1	0	34484
maltego.DNSNa...	iaoc.ietf.org	38	1	0	33182
maltego.DNSNa...	ops.ietf.org	38	1	0	20858
maltego.DNSNa...	mailarchive.ietf.org	38	1	0	15863
maltego.DNSNa...	trac.ietf.org	38	1	0	10822
maltego.DNSNa...	www.ops.ietf.org	38	1	0	10445
maltego.DNSNa...	ftp.ietf.org	38	1	0	10031
maltego.DNSNa...	lists.ietf.org	38	1	0	8103
maltego.DNSNa...	jabber.ietf.org	38	1	0	8068
maltego.DNSNa...	www2.ietf.org	38	1	0	5420
maltego.DNSNa...	search.ietf.org	38	1	0	2115
maltego.DNSNa...	odin.ietf.org	38	1	0	1664
maltego.DNSNa...	ia1.ietf.org	38	1	0	1253
maltego.DNSNa...	rsync.ietf.org	38	1	0	485
malteoo.DNSNa...	imap.ietf.ora	38	1	0	422

Output Transform Output

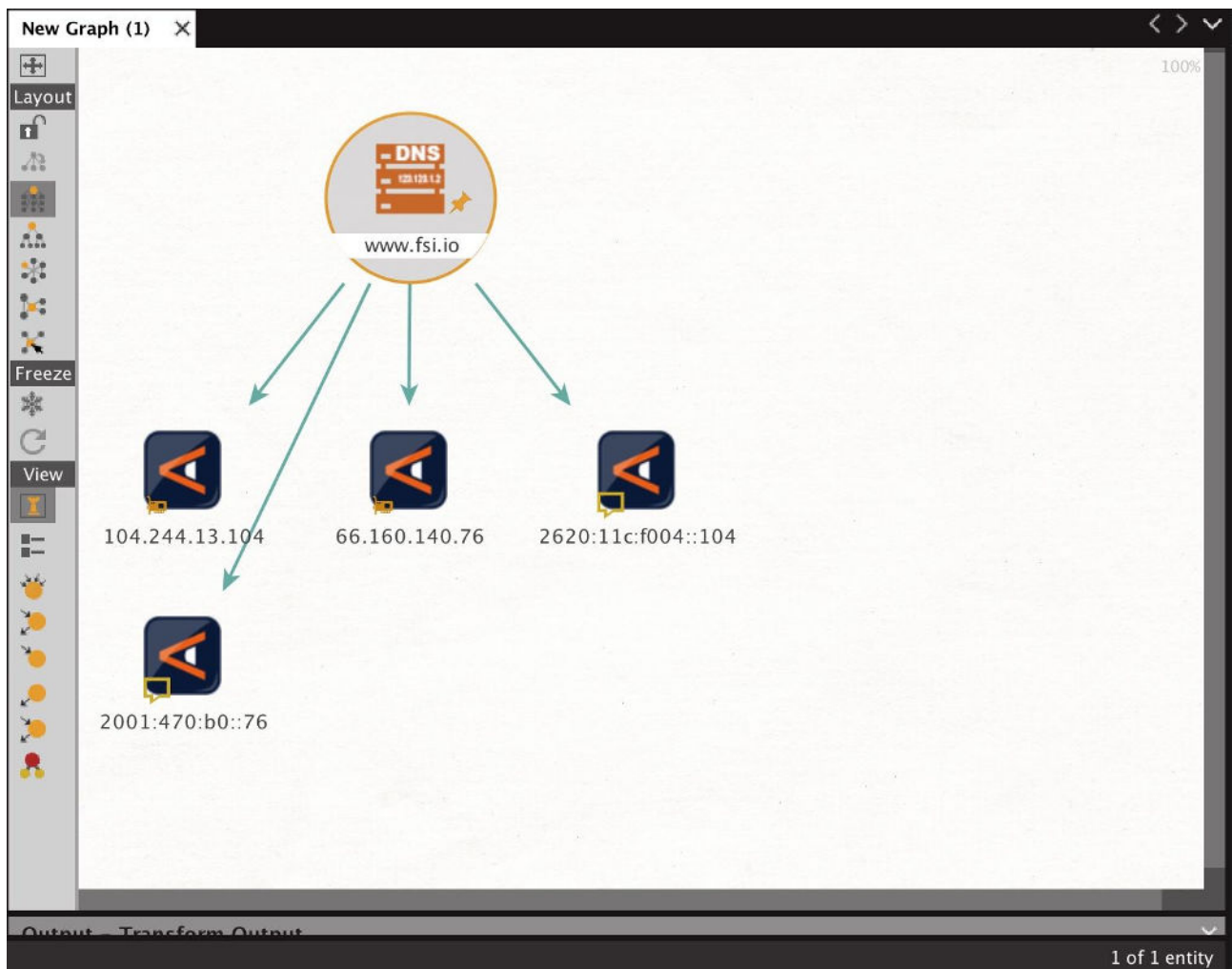
39 entities (2 nodes), 38 links (1 edge)

13. "To records with this hostname"

Name: paterva.v2.dnsdbrrsetDNSName

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

The screenshot displays the Maltego interface with a transform output table and a detail view for a specific entity.

Transform Output Table:

Type	Entity	Count	Score
maltego.DNSName	dns.cs.uoregon.edu	375	16983616
maltego.DNSName	ds1.cs.uoregon.edu	375	527804
maltego.DNSName	ds2.cs.uoregon.edu	375	524505
maltego.DNSName	galway.cs.uoregon.edu	375	224129
maltego.DNSName	planetlab3.cs.uoregon.edu	375	34904
maltego.Domain	cs.uoregon.edu	32	31834
maltego.DNSName	planetlab1.cs.uoregon.edu	375	28909
maltego.DNSName	planetlab4.cs.uoregon.edu	375	21004
maltego.DNSName	planetlab2.cs.uoregon.edu	375	20848
maltego.DNSName	dns2.cs.uoregon.edu	375	12708
maltego.DNSName	acm.cs.uoregon.edu	375	10712
maltego.DNSName	www.cs.uoregon.edu	375	10587
maltego.DNSName	cyrus.cs.uoregon.edu	375	10169
maltego.DNSName	issta2015.cs.uoregon.edu	375	8470
maltego.Domain	acm.cs.uoregon.edu	32	5742
maltego.DNSName	coglink.cs.uoregon.edu	375	5692
maltego.DNSName	mirage.cs.uoregon.edu	375	5524
maltego.DNSName	securityday.cs.uoregon.edu	375	4486

Output - Transform Output:

```
Running transform [DNSDB] Lookup *.$dnsname on 1 entities (from entity "cs.uoregon.edu")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname returned with 408 entities (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname done (from entity "cs.uoregon.edu")
```

Detail View:

DNS Name
maltego.DNSName
planetlab1.cs.uoregon.edu

Relationships

+ Incoming

- DNSDB Output

```
planetlab1.cs.uoregon.edu. IN A 128.223.8.111
planetlab1.cs.uoregon.edu. IN A 128.223.8.111
```

- DNSDB JSON Output

```
{'count': 825, 'time_first': 1283123184, 'rrtype': 'A', 'rrname': 'planetlab1.cs.uoregon.edu.', 'bailiwick': 'uoregon.edu.', 'rdata': '128.223.8.111', 'time_last': 1521254881}
{'count': 28909, 'time_first': 1278618020, 'rrtype': 'A', 'rrname': 'planetlab1.cs.uoregon.edu.', 'bailiwick': 'cs.uoregon.edu.', 'rdata': '128.223.8.111', 'time_last': 1521319630}
```

Generator detail

Source cs.uoregon.edu (DNS Name)
Transform [DNSDB] Lookup *.\$dnsname
Gen. date 2018-03-17 17:10:49.822 -0700

1 of 408 entities

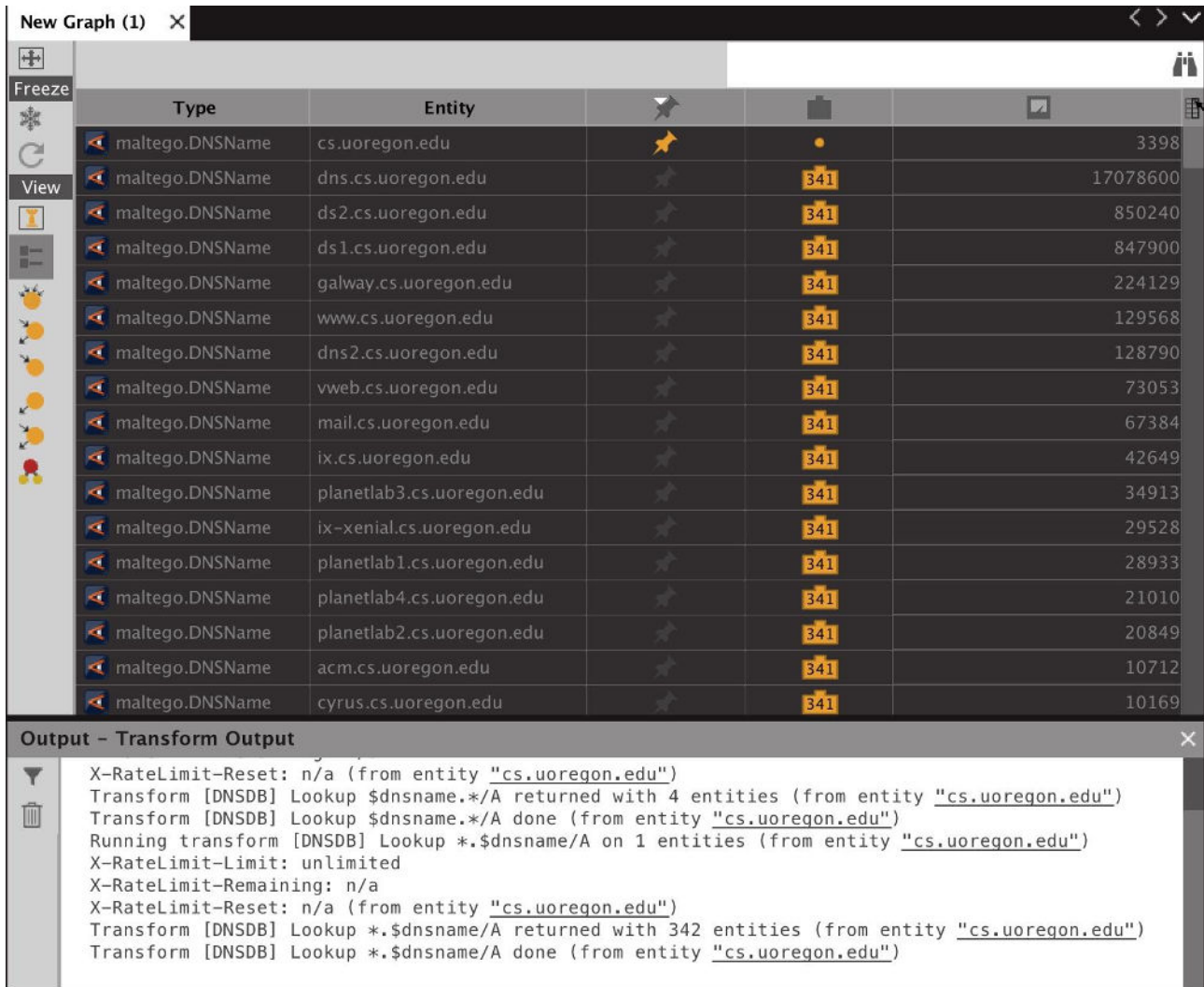
15. "Lookup *.\$dnsname/A"

Name: paterva.v2.dnsdbrrsetwclDNSNameA

Input Type: DNS Name

Input: cs.uoregon.edu

NOTE: DO NOT INCLUDE THE LEADING ASTERISK AND DOT IN THE SUPPLIED INPUT



The screenshot shows the Maltego interface with a transform output window open. The output window displays the following text:

```
X-RateLimit-Reset: n/a (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup $dnsname.*/* returned with 4 entities (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup $dnsname.*/* done (from entity "cs.uoregon.edu")
Running transform [DNSDB] Lookup *.$dnsname/A on 1 entities (from entity "cs.uoregon.edu")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname/A returned with 342 entities (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname/A done (from entity "cs.uoregon.edu")
```

Below the output window, a table of DNS records is visible. The table has the following columns: Type, Entity, and a numerical value. The records are as follows:

Type	Entity	Value
maltego.DNSName	cs.uoregon.edu	3398
maltego.DNSName	dns.cs.uoregon.edu	17078600
maltego.DNSName	ds2.cs.uoregon.edu	850240
maltego.DNSName	ds1.cs.uoregon.edu	847900
maltego.DNSName	galway.cs.uoregon.edu	224129
maltego.DNSName	www.cs.uoregon.edu	129568
maltego.DNSName	dns2.cs.uoregon.edu	128790
maltego.DNSName	vweb.cs.uoregon.edu	73053
maltego.DNSName	mail.cs.uoregon.edu	67384
maltego.DNSName	ix.cs.uoregon.edu	42649
maltego.DNSName	planetlab3.cs.uoregon.edu	34913
maltego.DNSName	ix-xenial.cs.uoregon.edu	29528
maltego.DNSName	planetlab1.cs.uoregon.edu	28933
maltego.DNSName	planetlab4.cs.uoregon.edu	21010
maltego.DNSName	planetlab2.cs.uoregon.edu	20849
maltego.DNSName	acm.cs.uoregon.edu	10712
maltego.DNSName	cyrus.cs.uoregon.edu	10169

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

The screenshot shows the Maltego interface with a transform output window and a detail view panel.

Transform Output:

```
Running transform [DNSDB] Lookup *.$dnsname/AAAA on 1 entities (from entity "cs.uoregon.edu")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname/AAAA returned with 44 entities (from entity "cs.uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname/AAAA done (from entity "cs.uoregon.edu")
```

Detail View:

DNS Name
maltego.DNSName
dns.cs.uoregon.edu

Relationships

+ Incoming

- DNSDB Output

```
dns.cs.uoregon.edu. IN AAAA 2001:468:d01:
dns.cs.uoregon.edu. IN AAAA 2001:468:d01:
dns.cs.uoregon.edu. IN AAAA 2001:468:d01:
dns.cs.uoregon.edu. IN AAAA 2001:468:d01:
```

- DNSDB JSON Output

```
{
  "count": 17,
  "time_first": 1397643051,
  "rrrtype": "AAAA",
  "rrname": "dns.cs.uoregon.edu.",
  "bailliwic": "",
  "rdata": "2001:468:d01:6::80df:609",
  "time_last": 1401247446
}

{
  "count": 4601,
  "time_first": 1387508027,
  "rrrtype": "AAAA",
  "rrname": "dns.cs.uoregon.edu.",
  "bailliwic": "edu.",
  "rdata": "2001:468:d01:6::80df:609",
  "time_last": 1521305838
}

{
  "count": 4294842,
  "time_first": 1277360055,
  "rrrtype": "AAAA",
  "rrname": "dns.cs.uoregon.edu.",
  "bailliwic": "uoregon.edu.",
  "rdata": "2001:468:d01:6::80df:609",
  "time_last": 1474553474
}
```

1 of 44 entities

17. "Lookup *.\$dnsname/CNAME"

Name: paterva.v2.dnsdbrrsetwclDNSNameCNAME

Input Type: DNS Name

Input: uoregon.edu

NOTE: DO NOT INCLUDE THE LEADING ASTERISK AND DOT IN THE SUPPLIED INPUT

The screenshot displays the Maltego interface with a 'New Graph (1)' window. The main table shows the results of a DNSDB lookup for the entity 'uoregon.edu'. The table has columns for Type, Entity, and a count of 6704. The entities listed include various subdomains like www.uoregon.edu, admissions.uoregon.edu, around.uoregon.edu, giving.uoregon.edu, financialaid.uoregon.edu, sync.uoregon.edu, mirror.nic.uoregon.edu, gradschool.uoregon.edu, visit.uoregon.edu, housing.uoregon.edu, business.uoregon.edu, mappinghistory.uoregon.edu, and uonews.uoregon.edu.

The 'Output - Transform Output' window shows the following text:

```
Running transform [DNSDB] Lookup *.$dnsname/CNAME on 1 entities (from entity "uoregon.edu")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname/CNAME returned with 6704 entities (from entity "uoregon.edu")
Transform [DNSDB] Lookup *.$dnsname/CNAME done (from entity "uoregon.edu")
```

The 'Detail View' window shows the selected entity 'www.uoregon.edu' with its relationships and DNSDB output. The DNSDB output includes the following JSON:

```
{
  "count": 1002955,
  "time_first": 1378997049,
  "rrrtype": "CNAME",
  "rrname": "www.uoregon.edu.",
  "bailiwick": "uoregon.edu.",
  "rdata": "wc-www.uoregon.edu.",
  "time_last": 1419869697
}
{
  "count": 1924809,
  "time_first": 1287490359,
  "rrrtype": "CNAME",
  "rrname": "www.uoregon.edu.",
  "bailiwick": "uoregon.edu.",
  "rdata": "uowc-www.uoregon.edu.",
  "time_last": 1378997036
}
{
  "count": 1241361,
  "time_first": 1419869370,
  "rrrtype": "CNAME",
  "rrname": "www.uoregon.edu.",
  "bailiwick": "uoregon.edu.",
  "rdata": "drupal-cluster5.uoregon.edu.",
  "time_last": 1521335602
}
```

The 'Generator detail' window shows the source 'uoregon.edu (DNS Name)' and the transform '[DNSDB] Lookup *.\$dnsname/CNAME'.

1 of 6705 entities

18. "Lookup \$dnsname.*"

Name: paterva.v2.dnsdbrrsetwcrDNSName

Input Type: DNS Name

Input: uoregon

NOTE: DO NOT INCLUDE THE TRAILING DOT AND ASTERISK IN THE SUPPLIED INPUT

The screenshot shows the Maltego interface with a graph titled "New Graph (1)". The graph contains several entities of type "maltego.DNSName" and one "maltego.Domain" entity. The entities are listed in a table below:

Type	Entity	Count	Score	Other
maltego.DNSName	uoregon	0	839	0
maltego.Domain	uoregon.edu	53	1	2495910
maltego.DNSName	uoregon.sharepoint.com	786	1	19514
maltego.DNSName	uoregon.orgsync.com	786	1	14220
maltego.DNSName	uoregon.kappa.org	786	1	11872
maltego.DNSName	uoregon.medicatconnect.com	786	1	8830
maltego.DNSName	uoregon.academicworks.com	786	1	7748
maltego.DNSName	uoregon.interactyx.com	786	1	7234
maltego.DNSName	uoregon.collegescheduler.com	786	1	5932
maltego.DNSName	uoregon.mhcampus.com	786	1	4004
maltego.DNSName	uoregon.tridelta.org	786	1	3192
maltego.DNSName	uoregon.edu	786	1	2421
maltego.DNSName	uoregon.kappadelta.org	786	1	1979
maltego.DNSName	uoregon.imodules.com	786	1	1876
maltego.DNSName	uoregon.us2.list-manage.com	786	1	1790
maltego.DNSName	uoregon.sidearmsports.com	786	1	1365
maltego.DNSName	uoregon.libapps.com	786	1	1207
maltego.DNSName	uoregon.us2.list-manage1.com	786	1	1158
maltego.DNSName	uoregon.edu.education2020.us	786	1	1106

The "Output - Transform Output" window shows the following text:

```
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.* returned with 839 entities (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.* done (from entity "uoregon")
```

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

The screenshot displays the Maltego interface. The main window shows a list of entities under the 'Type' column, all of which are 'maltego.DNSName' and point to various domains under the 'Entity' column. The 'Output - Transform Output' window shows the following text:

```
Running transform [DNSDB] Lookup $dnsname.* /A on 1 entities (from entity "uoregon")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.* /A returned with 432 entities (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.* /A done (from entity "uoregon")
```

The 'Detail View' window shows the selected entity: 'uoregon.studentaidcalculator.com'. It displays relationships, incoming links, and DNSDB output. The DNSDB output shows two records:

```
uoregon.studentaidcalculator.com. IN A 38.111.41.7:
uoregon.studentaidcalculator.com. IN A 65.74.151.20
```

The DNSDB JSON output shows the following JSON objects:

```
{
  "count": 12,
  "time_first": 1394165073,
  "rrtype": "A",
  "rrname": "uoregon.studentaidcalculator.com",
  "bailiwick": "studentaidcalculator.com",
  "rdata": "38.111.41.72",
  "time_last": 1394177441
}
{
  "count": 54906,
  "time_first": 1315590061,
  "rrtype": "A",
  "rrname": "uoregon.studentaidcalculator.com",
  "bailiwick": "studentaidcalculator.com",
  "rdata": "65.74.151.20",
  "time_last": 1505790545
}
```

The 'Generator detail' window shows the following information:

```
Source: uoregon (DNS Name)
Transform: [DNSDB] Lookup $dnsname.* /A
Gen. date: 2018-03-17 20:16:15.90 -0700
```

The bottom right corner of the interface indicates '1 of 433 entities'.

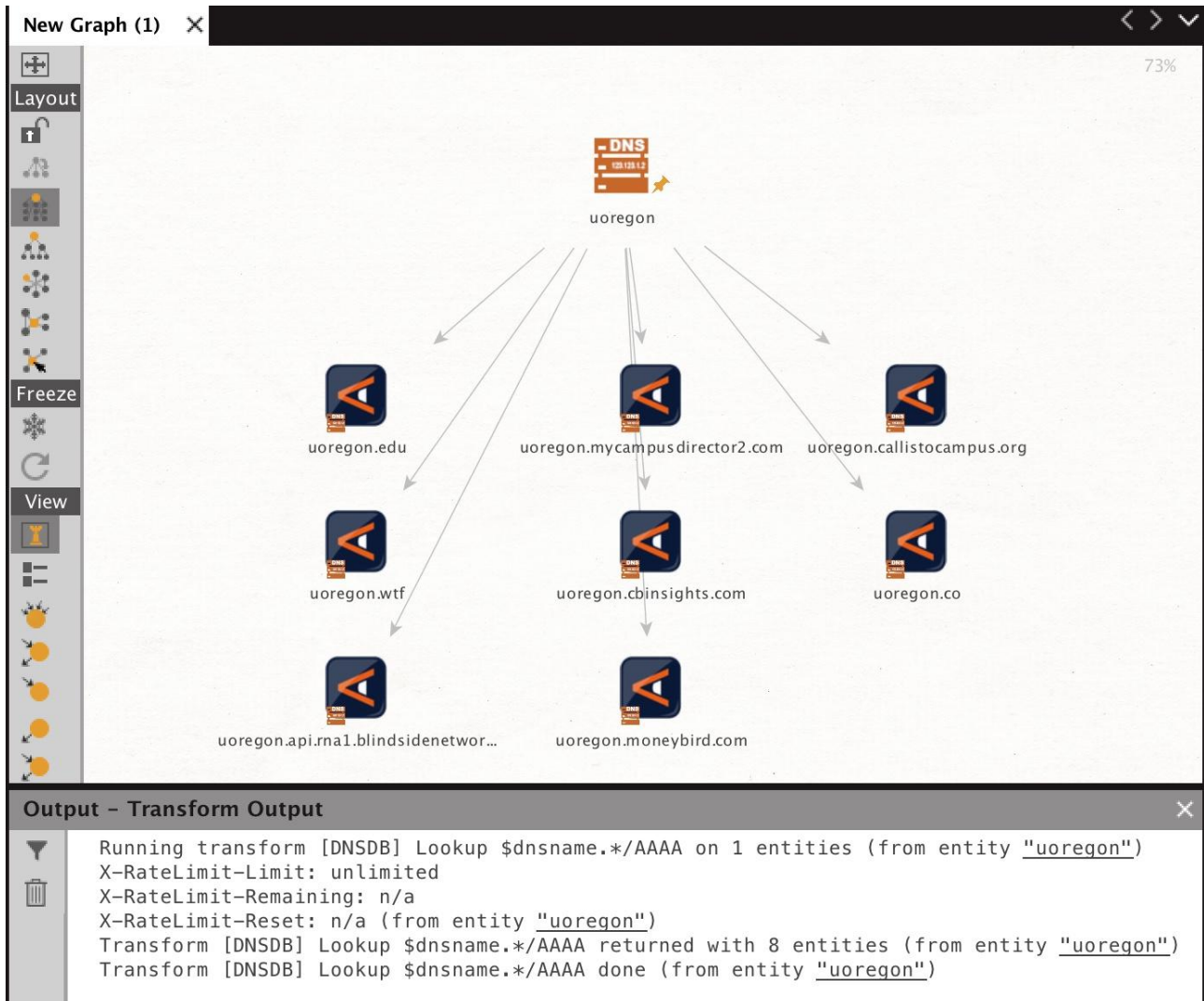
20. "Lookup \$dnsname.*/AAAA"

Name: paterva.v2.dnsdbrrsetwcrDNSNameAAAA

Input Type: DNS Name

Input: uoregon

NOTE: DO NOT INCLUDE THE TRAILING DOT AND ASTERISK IN THE SUPPLIED INPUT



The screenshot displays the Maltego interface with a new graph titled "New Graph (1)". The graph shows a central node labeled "uoregon" with a DNS icon. Eight arrows point from this node to child nodes, each with a DNS icon and a domain name: "uoregon.edu", "uoregon.wtf", "uoregon.api.rna1.blindsidenetwor...", "uoregon.mycampusdirector2.com", "uoregon.cbinsights.com", "uoregon.moneybird.com", "uoregon.callistocampus.org", and "uoregon.co". The interface includes a sidebar with "Layout", "Freeze", and "View" sections. The bottom pane, titled "Output - Transform Output", shows the following text:

```
Running transform [DNSDB] Lookup $dnsname.*/AAAA on 1 entities (from entity "uoregon")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.*/AAAA returned with 8 entities (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.*/AAAA done (from entity "uoregon")
```


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

The screenshot shows the Maltego interface with a graph of entities and a detail view. The graph lists various DNSName entities under the 'maltego.DNSName' type, all originating from the 'uoregon' entity. The detail view shows the selected entity 'uoregon.sharepoint.com' and its relationships, including DNSDB output and JSON output.

Type	Entity	Count	Score
maltego.DNSName	uoregon	0	
maltego.DNSName	uoregon.spoonuniversity.com	346	166054
maltego.DNSName	uoregon.sharepoint.com	346	19628
maltego.DNSName	uoregon.kappa.org	346	11892
maltego.DNSName	uoregon.collegescheduler.com	346	5933
maltego.DNSName	uoregon.mhcampus.com	346	4004
maltego.DNSName	uoregon.tridelta.org	346	3192
maltego.DNSName	uoregon.kappadelta.org	346	1979
maltego.DNSName	uoregon.imodules.com	346	1876
maltego.DNSName	uoregon.us2.list-manage.com	346	1798
maltego.DNSName	uoregon.us2.list-manage1.com	346	1158
maltego.DNSName	uoregon.instructure.com	346	846
maltego.DNSName	uoregon.hosted.panopto.com	346	842
maltego.DNSName	uoregon.us2.list-manage2.com	346	769
maltego.DNSName	uoregon.libcal.com	346	677
maltego.DNSName	uoregon.myonlinecamp.com	346	651
maltego.DNSName	uoregon.goldenkey.org	346	596

Detail View: uoregon.sharepoint.com

- Relationships**
 - Incoming**
 - DNSDB Output**
 - uoregon.sharepoint.com. IN CNAME prodnet296-253
 - uoregon.sharepoint.com. IN CNAME prodnet296-253
 - DNSDB JSON Output**
 - { "count": 10811, "time_first": 1431563656, "rrtype": "CNAME", "rrname": "uoregon.sharepoint.com.", "bailiwick": "sharepoint.com.", "rdata": "prodnet296-253a0000.sharepointonline.com.akadn", "time_last": 1486445206 }
 - { "count": 19628, "time_first": 1486254008, "rrtype": "CNAME", "rrname": "uoregon.sharepoint.com.", "bailiwick": "sharepoint.com.", "rdata": "prodnet296-253edgea0000.sharepointonline.com.a", "time_last": 1521331917 }
 - Generator detail**
 - Source**: uoregon (DNS Name)
 - Transform**: [DNSDB] Lookup \$dnsname.*/CNAME
 - Gen. date**: 2018-03-17 20:26:21.918 -0700

Output - Transform Output

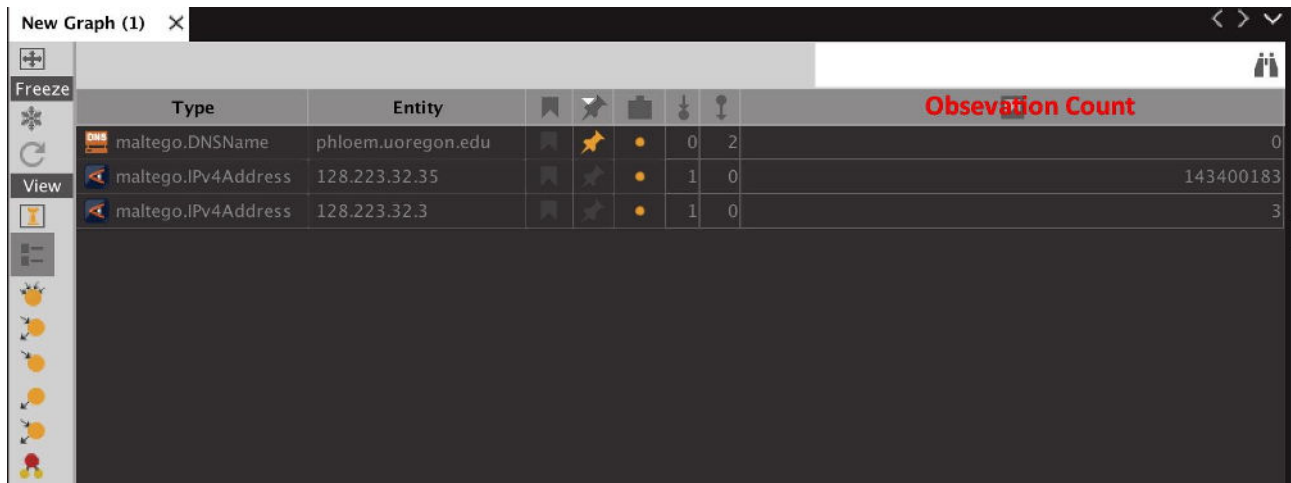
```
Running transform [DNSDB] Lookup $dnsname.*/CNAME on 1 entities (from entity "uoregon")
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.*/CNAME returned with 346 entities (from entity "uoregon")
Transform [DNSDB] Lookup $dnsname.*/CNAME done (from entity "uoregon")
```

22. "To A Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToA

Input Type: DNS Name

Input: phloem.uoregon.edu



The screenshot shows the Maltego interface with a table of results for the query "To A Records for this DNSName". The table has columns for Type, Entity, and Observation Count. The results are as follows:

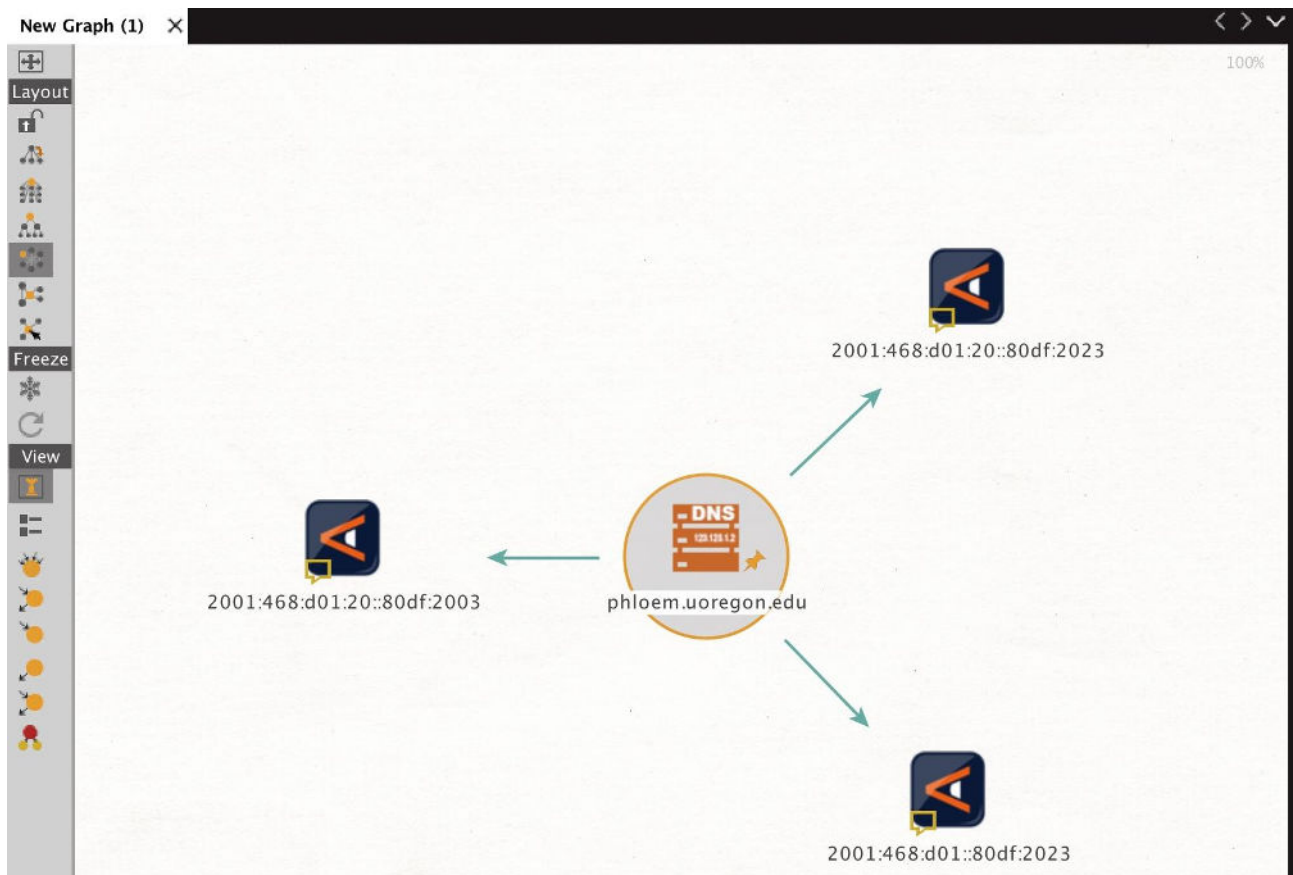
Type	Entity	Observation Count
maltego.DNSName	phloem.uoregon.edu	0
maltego.IPv4Address	128.223.32.35	143400183
maltego.IPv4Address	128.223.32.3	3

23. "To AAAA Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToAAAA

Input Type: DNS Name

Input: phloem.uoregon.edu

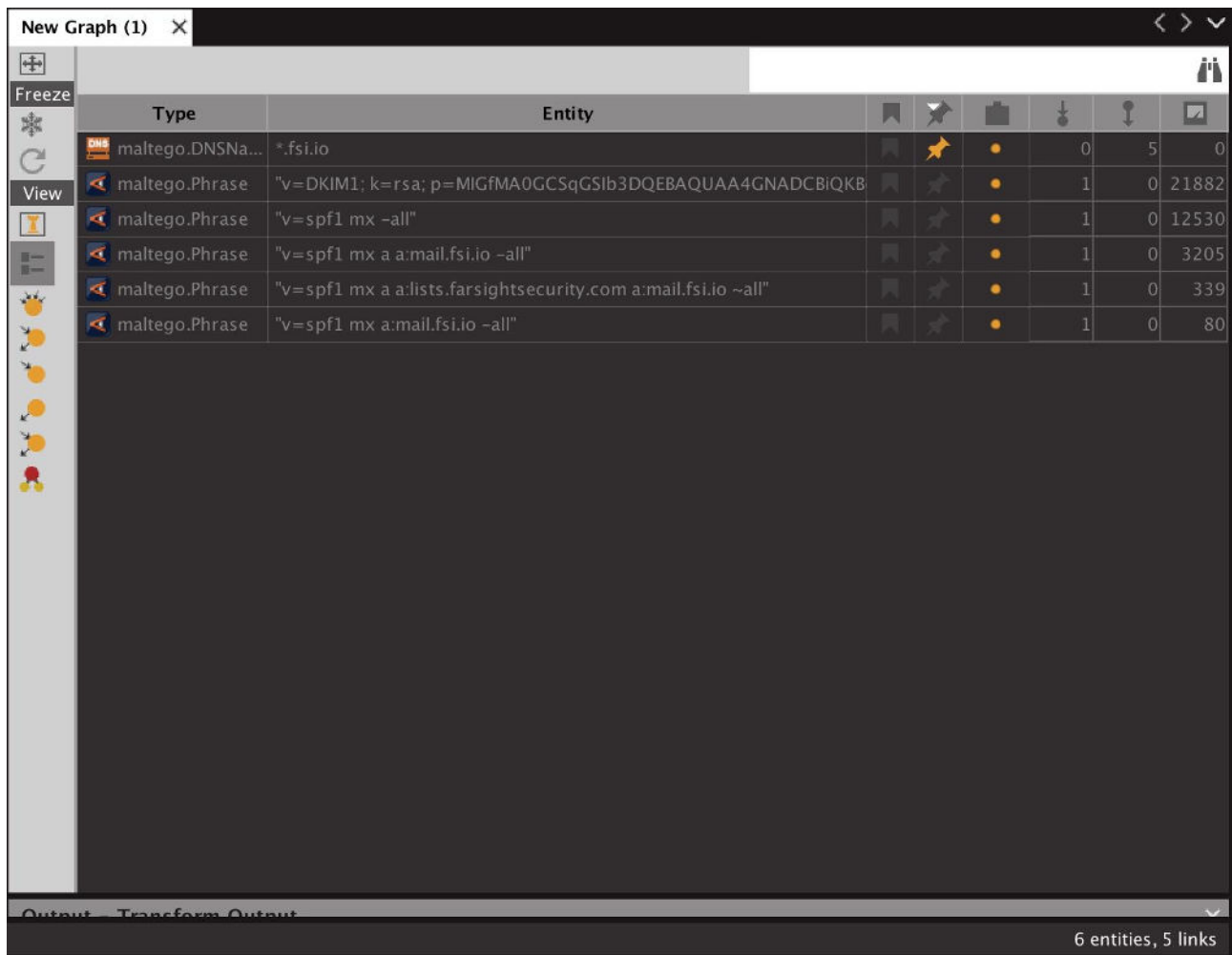


24. "To TXT Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToTXT

Input Type: DNS Name

Input: *.fsi.io



The screenshot shows the Maltego interface with a graph titled "New Graph (1)". The graph contains 6 entities and 5 links. The entities are listed in a table below:

Type	Entity	Count
maltego.DNSName	*.fsi.io	5
maltego.Phrase	"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB...	21882
maltego.Phrase	"v=spf1 mx -all"	12530
maltego.Phrase	"v=spf1 mx a a:mail.fsi.io -all"	3205
maltego.Phrase	"v=spf1 mx a a:lists.farsightsecurity.com a:mail.fsi.io ~all"	339
maltego.Phrase	"v=spf1 mx a:mail.fsi.io -all"	80

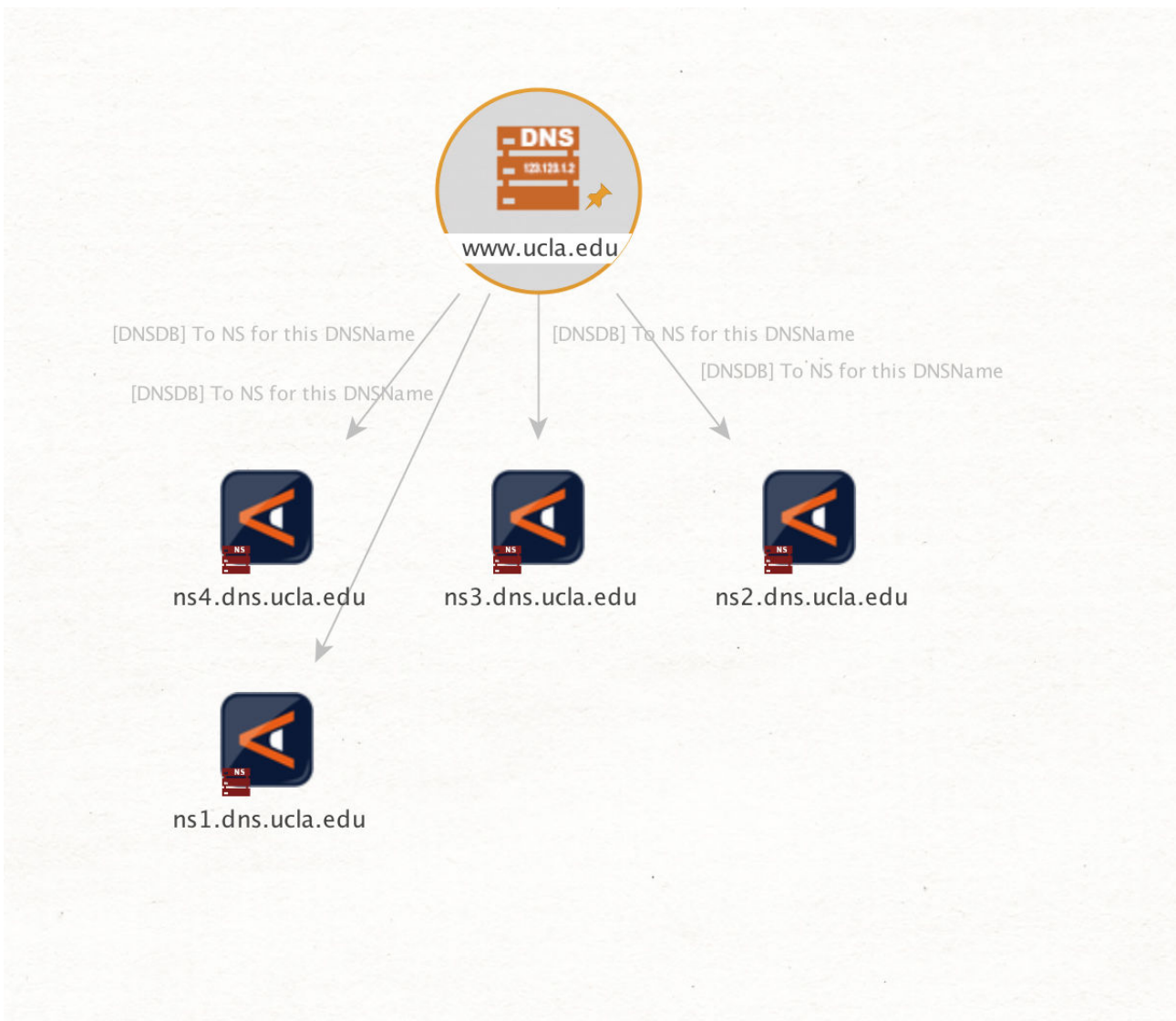
Output: Transform Output
6 entities, 5 links

25. "To NS for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToNS

Input Type: DNS Name

Input: www.ucla.edu

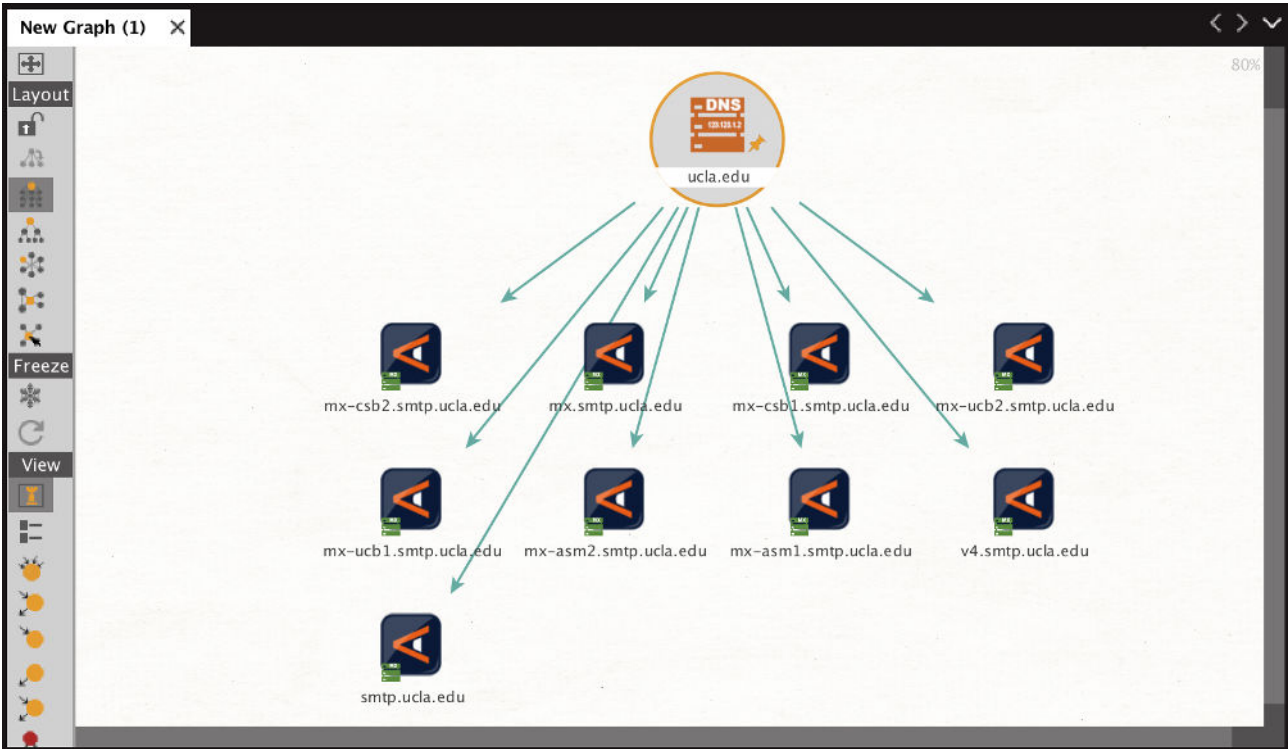


26. "To MX for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToMX

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

Type	Entity	Score	Weight	Count	Value
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102594 10800 3600 2419200 900	50	1	0	3300058
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102556 10800 3600 2419200 900	50	1	0	3259710
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102589 10800 3600 2419200 900	50	1	0	2019697
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102553 10800 3600 2419200 900	50	1	0	1986022
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102592 10800 3600 2419200 900	50	1	0	1317424
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102571 10800 3600 2419200 900	50	1	0	1080771
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102563 10800 3600 2419200 900	50	1	0	970263
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102574 10800 3600 2419200 900	50	1	0	900387
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102575 10800 3600 2419200 900	50	1	0	865593
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102565 10800 3600 2419200 900	50	1	0	691554
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102591 10800 3600 2419200 900	50	1	0	537571
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102559 10800 3600 2419200 900	50	1	0	333648
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102586 10800 3600 2419200 900	50	1	0	283641
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102551 10800 3600 2419200 900	50	1	0	140238
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102555 10800 3600 2419200 900	50	1	0	134850
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102545 10800 3600 2419200 900	50	1	0	127556
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102544 10800 3600 2419200 900	50	1	0	109054
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102554 10800 3600 2419200 900	50	1	0	80584
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102549 10800 3600 2419200 900	50	1	0	78933
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102578 10800 3600 2419200 900	50	1	0	70073
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102561 10800 3600 2419200 900	50	1	0	16711
maltego.Phrase	ns1.dns.ucla.edu. hostmaster.ucla.edu. 2012102576 10800 3600 2419200 900	50	1	0	14292

Output: Transform Output

51 entities (2 nodes), 50 links (1 edge)

28. "To SRV Records for this DNSName"

Name: paterva.v2.dnsdbrrsetDNSNameToSRV

Input Type: DNS Name

Input: *.fsi.io

The screenshot shows the Maltego interface for a new graph. The main area displays a table of entities and their relationships. The table has columns for Type, Entity, and several numerical values. The entities are as follows:

Type	Entity	Value 1	Value 2	Value 3	Value 4	Value 5
maltego.DNSName	*.fsi.io			0	5	0
maltego.Phrase	5 0 5222 im.fsi.io			1	0	24530
maltego.Phrase	5 0 3478 im.fsi.io			1	0	2540
maltego.Phrase	5 0 5269 im.fsi.io			1	0	2306
maltego.Phrase	100 100 993 hq.fsi.io			1	0	2
maltego.Phrase	100 100 443 hq.fsi.io			1	0	1

At the bottom of the interface, a status bar indicates "6 entities, 5 links".

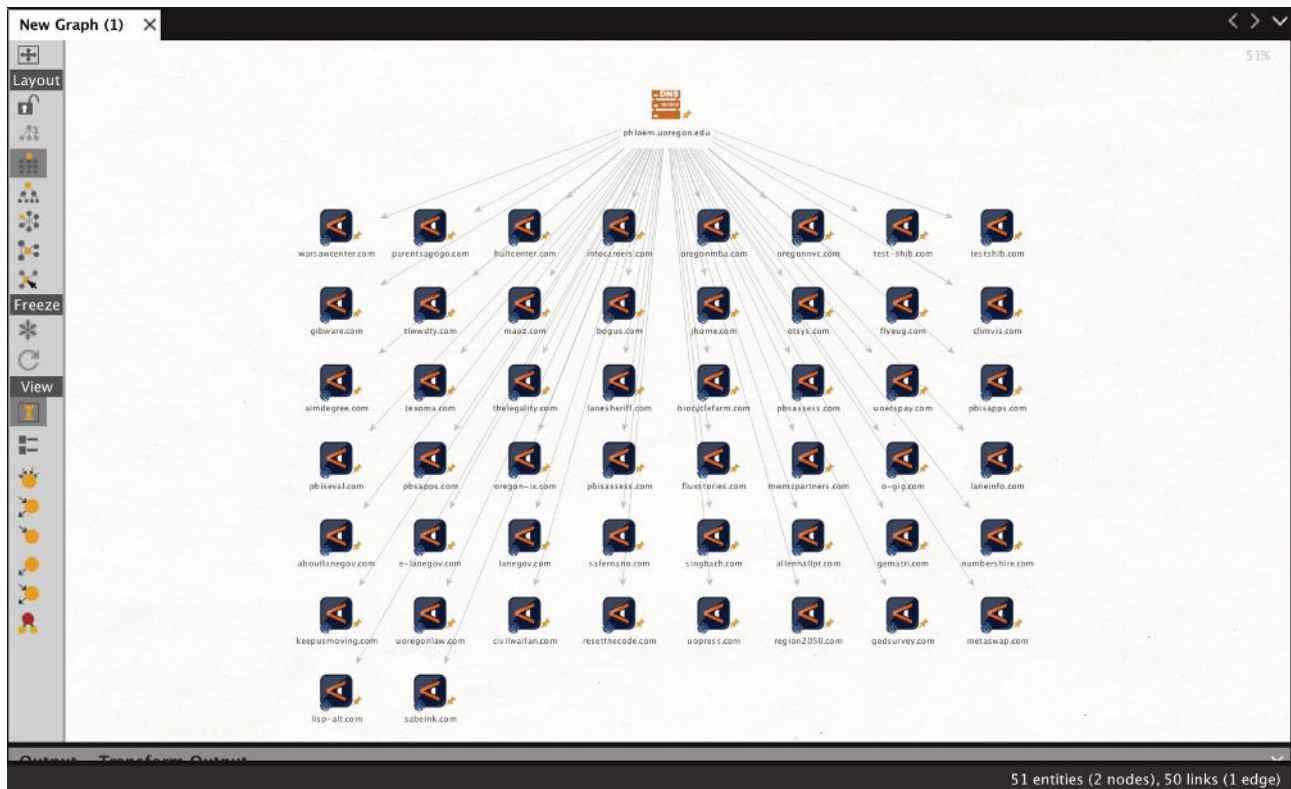
29. "Records with this value"

Name: paterva.v2.dnsdbdataDNSName

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.dnsdbdataMXType

Input Type: DNS Name

Input: microsoft-com.mail.protection.outlook.com

Limited to: MX records

List view

The screenshot displays the Maltego interface for a graph titled "New Graph (1)". The main table shows the following data:

Type	Entity	Score	Links	Outgoing	Incoming	Weight
maltego.DNSName	microsoft-com.mail.protection.outlook.com	0	27	0	27	0
maltego.Domain	microsoft.com	27	1	0	0	3995176
maltego.Domain	office365.microsoft.com	27	1	0	0	56579
maltego.Domain	email.teams.microsoft.com	27	1	0	0	6177
maltego.Domain	mail.windowsazure.com	27	1	0	0	5869
maltego.Domain	pininfarina.se	27	1	0	0	4633
maltego.Domain	messages.microsoft.com	27	1	0	0	3727
maltego.Domain	mail.microsoftazure.com	27	1	0	0	1700
maltego.Domain	service.microsoft.com	27	1	0	0	1171
maltego.Domain	corp.microsoft.com	27	1	0	0	393
maltego.Domain	cloudyn.com	27	1	0	0	192
maltego.Domain	altvr.com	27	1	0	0	171

The "Output - Transform Output" pane shows the following text:

```
X-RateLimit-Limit: unlimited
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "microsoft-com.mail.protection.ou...")
Transform [DNSDB] Domains using this MX returned with 27 entities (from entity "microsoft-com.mail.protection.ou...")
Transform [DNSDB] Domains using this MX done (from entity "microsoft-com.mail.protection.ou...")
```

At the bottom right of the interface, it states: "28 entities (2 nodes), 27 links (1 edge)".

31. "Domains Using This NS"

Name: paterva.v2.dnsdbdataNSType

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

The screenshot shows the Maltego interface with a graph titled "New Graph (1)". The graph contains a table with the following data:

Type	Entity	Count
maltego.DNSName	phloem.uoregon.edu	0
maltego.Domain	atlasofyellowstone.com	2871
maltego.Domain	atlasyellowstone.com	2871
maltego.Domain	bogus.com	2871
maltego.Domain	climvis.com	2871
maltego.Domain	corvallispermits.com	2871
maltego.Domain	eugeneairport.com	2871
maltego.Domain	flyeug.com	2871
maltego.Domain	gibware.com	2871
maltego.Domain	hultcenter.com	2871
maltego.Domain	imageendriver.com	2871
maltego.Domain	intocareers.com	2871
maltego.Domain	jhome.com	2871
maltego.Domain	maoz.com	2871
maltego.Domain	mychildsfuture.com	2871
maltego.Domain	oregonmba.com	2871

Below the table is an "Output - Transform Output" window showing the following text:

```
X-RateLimit-Reset: n/a (from entity "phloem.uoregon.edu")
Transform [DNSDB] Domains using this NS returned with 257 entities (fr
Transform [DNSDB] Domains using this NS done (from entity "phloem.uore
```

32. "Lookup *.\$phrase"

Name: paterva.v2.dnsdbrrsetwclPhrase
 Input Type: Phrase
 Input: eou.edu
 Only selected columns shown

The screenshot shows the Maltego interface with a table of entities and a detail view for the selected entity 'www.eou.edu'.

Type	Entity	Count	Score
maltego.Phrase	eou.edu	0	
maltego.DNSName	ns2.eou.edu	668066	2637
maltego.DNSName	ns1.eou.edu	478448	2637
maltego.Domain	eou.edu	248380	
maltego.DNSName	ns.eou.edu	202421	2637
maltego.DNSName	harris.eou.edu	98788	2637
maltego.DNSName	chinook.eou.edu	64588	2637
maltego.DNSName	www.eou.edu	57674	2637
maltego.DNSName	gmail.eou.edu	29206	2637
maltego.DNSName	snake.eou.edu	24164	2637
maltego.DNSName	my.eou.edu	23326	2637
maltego.DNSName	pierce.eou.edu	21271	2637
maltego.DNSName	mx02.eou.edu	15615	2637
maltego.DNSName	blackboard4.eou.edu	15439	2637
maltego.DNSName	mx01.eou.edu	15106	2637

Detail View for www.eou.edu

- DNS Name:** maltego.DNSName, www.eou.edu
- Relationships:**
 - Incoming:**
 - DNSDB Output:** www.eou.edu. IN CNAME eou.edu., www.eou.edu. IN CNAME harris.eou.edu.
 - DNSDB JSON Output:**

```
{
  "count": 405757,
  "time_first": 1310000159,
  "rrtype": "CNAME",
  "rrname": "www.eou.edu.",
  "bailiwick": "eou.edu.",
  "rdata": "eou.edu.",
  "time_last": 1521239889
}
```

```
{
  "count": 57674,
  "time_first": 1277414228,
  "rrtype": "CNAME",
  "rrname": "www.eou.edu.",
  "bailiwick": "eou.edu.",
  "rdata": "harris.eou.edu.",
  "time_last": 1309999679
}
```
 - Generator detail:**
 - Source:** eou.edu (Phrase)
 - Transform:** [DNSDB] Lookup *.\$phrase
 - Gen. date:** 2018-03-16 15:53:30.690 -0700

Output - Transform Output

```
X-RateLimit-Remaining: n/a
X-RateLimit-Reset: n/a (from entity "eou.edu")
Transform [DNSDB] Lookup *.$phrase returned with 2644 entities (
Transform [DNSDB] Lookup *.$phrase done (from entity "eou.edu")
```

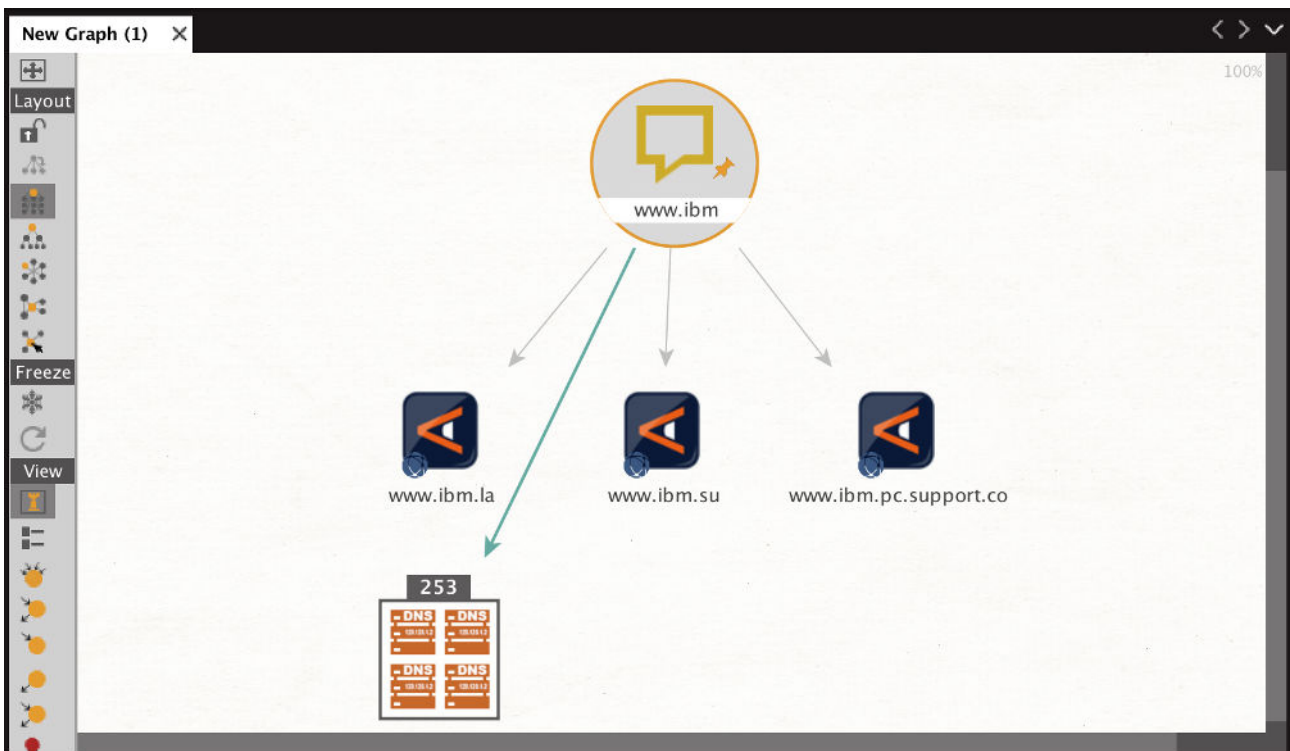
1 of 2645 entities

33. "lookup \$phrase.*"

Name: paterva.v2.dnsdbrrsetwcrPhrase

Input Type: Phrase

Input: www.ibm

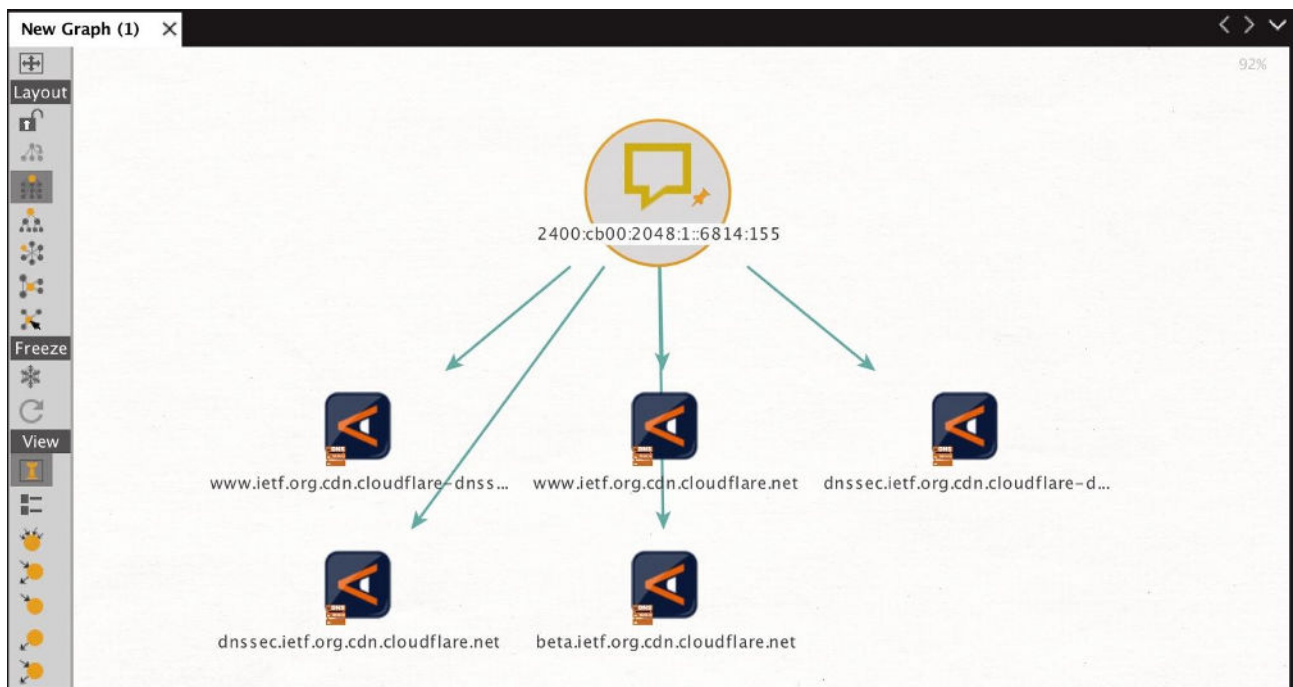


34. "To DNSNames from this IPv6 Address"

Name: paterva.v2.dnsdbrdatalIPv6Address

Input Type: Phrase

Input: 2400:cb00:2048:1::6814:155

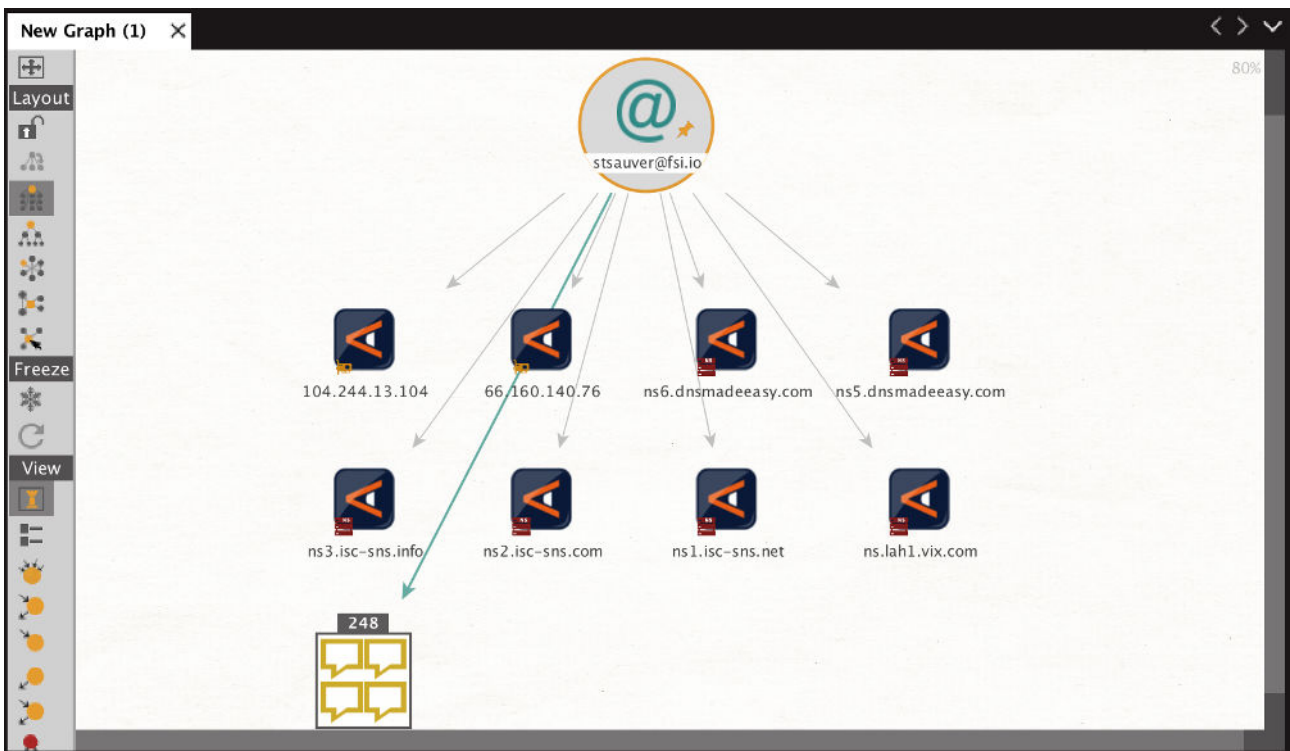


35. "To DNSNames from this email"

Name: paterva.v2.dnsdbrrsetEmail

Input Type: Email address

Input: stsauver@fsi.io



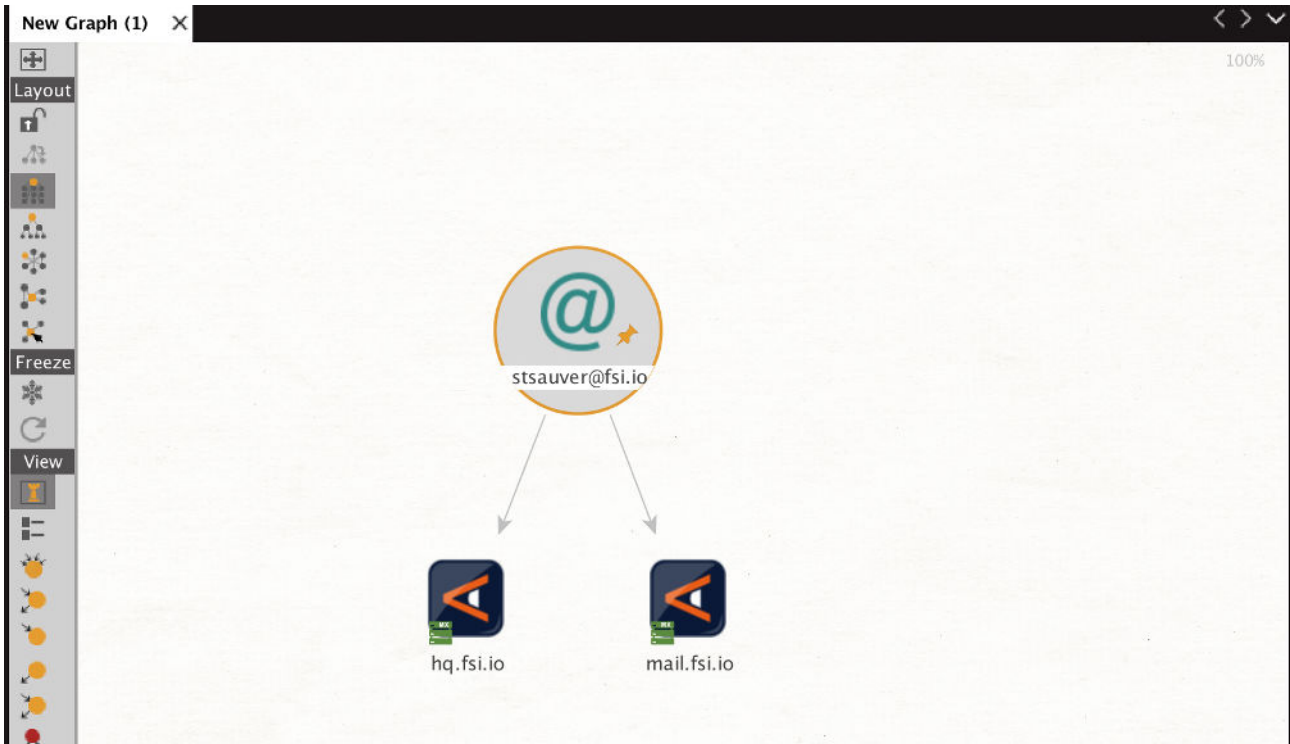
36. "MX from E-mail address"

Name: paterva.v2.dnsdbrrsetEmailMX

Input Type: Email address

Input: stsauver@fsi.io

Results limited to no more than 12 results for the purposes of this example

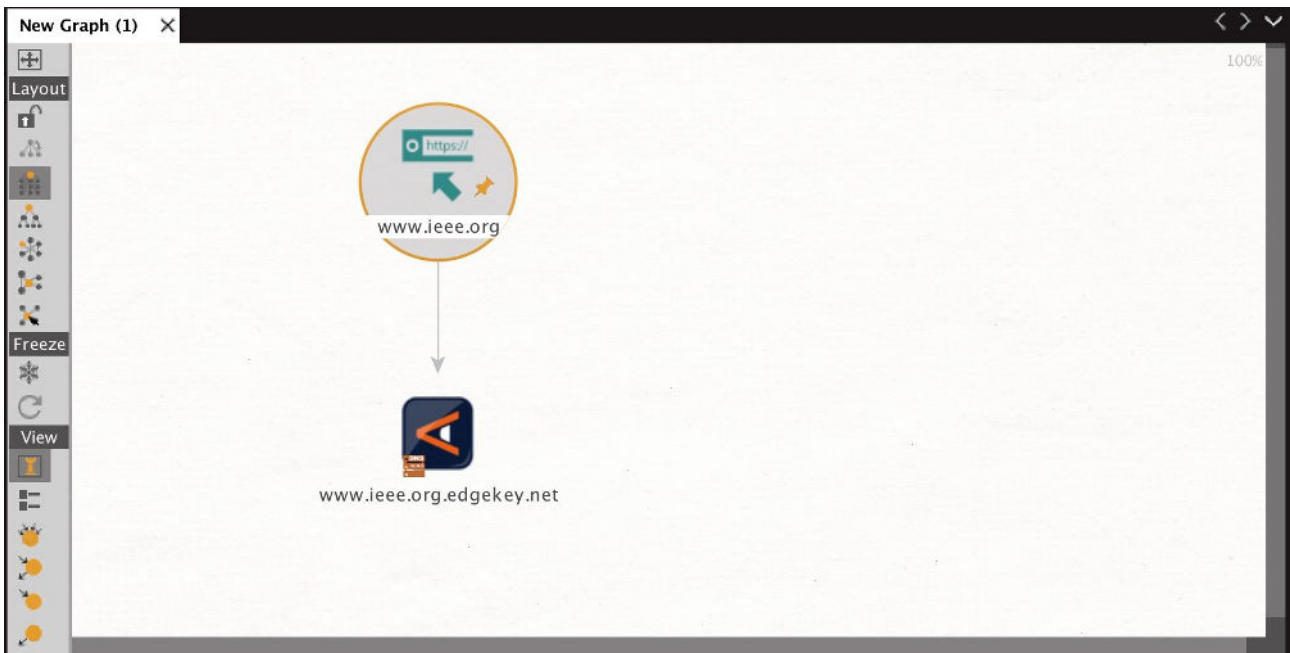


37. "To DNSNames from this URL"

Name: paterva.v2.dnsdbrrsetURL

Input Type: URL

Input: <https://www.ieee.org/>

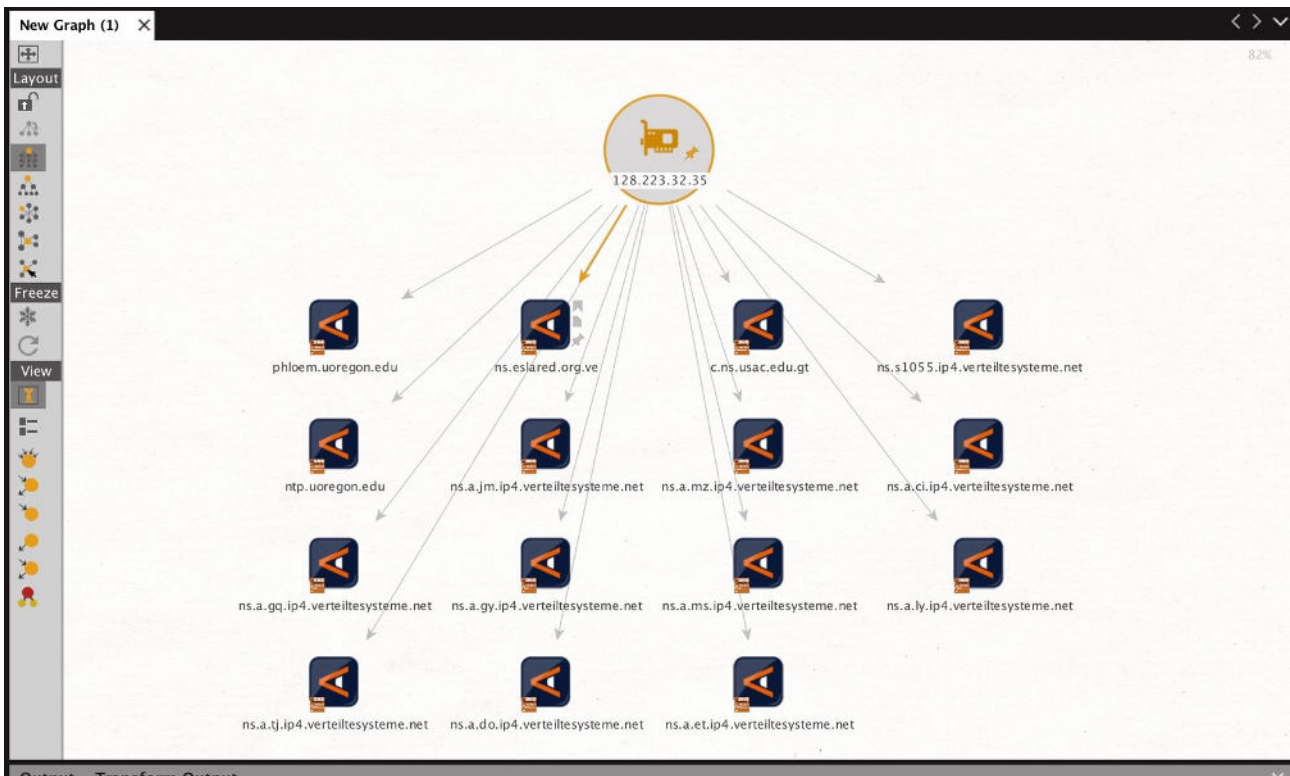


38. "To DNSNames with this IP"

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.

The screenshot shows the Maltego interface with a table of results. The table has columns for Type, Entity, and several numerical columns. The results are as follows:

Type	Entity	28	1	0	374333981
maltego.DNSName	phloem.uoregon.edu	28	1	0	374333981
maltego.DNSName	ns.eslared.org.ve	28	1	0	224589
maltego.DNSName	c.ns.usac.edu.gt	28	1	0	58762
maltego.DNSName	wpad.uoregon.edu	28	1	0	1829
maltego.DNSName	ns1.uoregon.edu	28	1	0	1445
maltego.DNSName	ns.s1055.ip4.verteiltesysteme.net	28	1	0	1034
maltego.DNSName	ntp.uoregon.edu	28	1	0	626
maltego.DNSName	proxy1.uoregon.edu	28	1	0	214
maltego.DNSName	adns.uoregon.edu	28	1	0	50
maltego.DNSName	ns.a.jm.ip4.verteiltesysteme.net	28	1	0	43
maltego.DNSName	ns.a.mz.ip4.verteiltesysteme.net	28	1	0	41
maltego.DNSName	proxy.uoregon.edu	28	1	0	40
maltego.DNSName	ns.a.ci.ip4.verteiltesysteme.net	28	1	0	37
maltego.DNSName	ns.a.gq.ip4.verteiltesysteme.net	28	1	0	36
maltego.DNSName	ns.a.gy.ip4.verteiltesysteme.net	28	1	0	35
maltego.DNSName	ns.a.ly.ip4.verteiltesysteme.net	28	1	0	35
maltego.DNSName	ns.a.ms.ip4.verteiltesysteme.net	28	1	0	35
maltego.DNSName	ns.a.do.ip4.verteiltesysteme.net	28	1	0	33
maltego.DNSName	ns.a.tj.ip4.verteiltesysteme.net	28	1	0	33
maltego.DNSName	ns.a.et.ip4.verteiltesysteme.net	28	1	0	31
maltego.DNSName	rad2.uoregon.edu	28	1	0	11
maltego.DNSName	athletics-wireless-vpn.uoregon.edu	28	1	0	5

Output: Transform Output
29 entities (2 nodes), 28 links (1 edge)