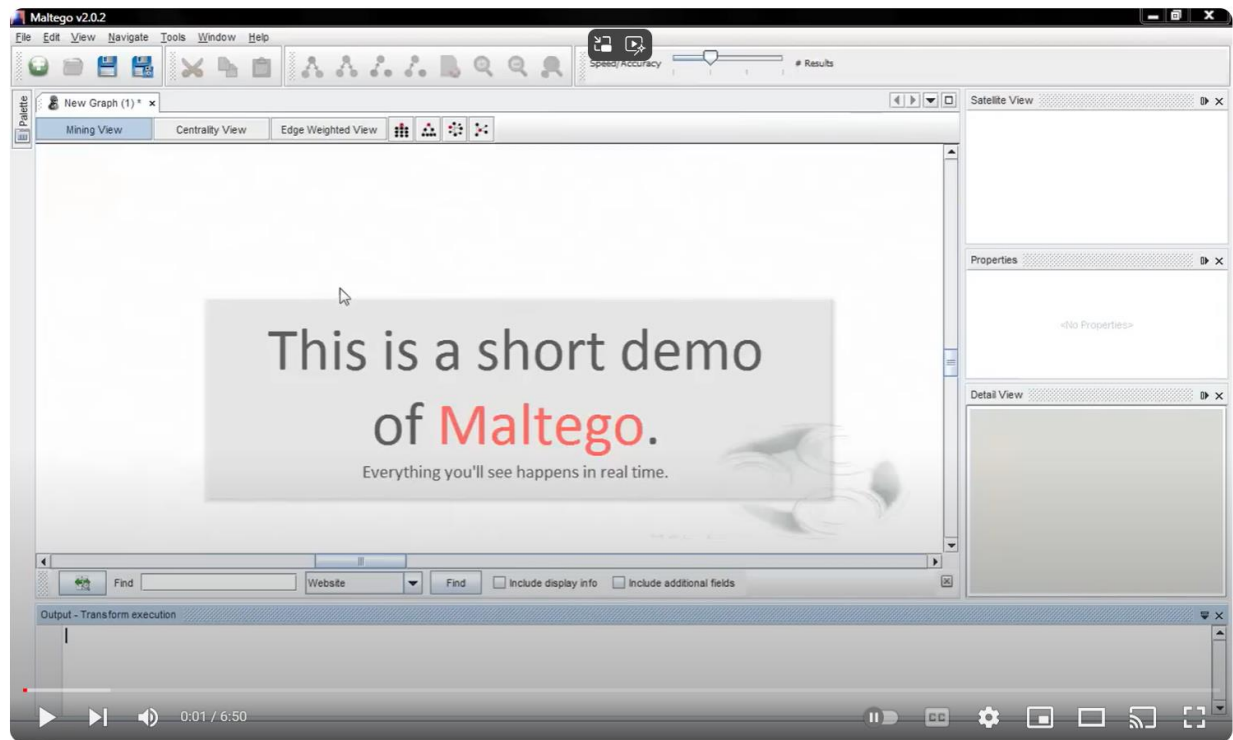
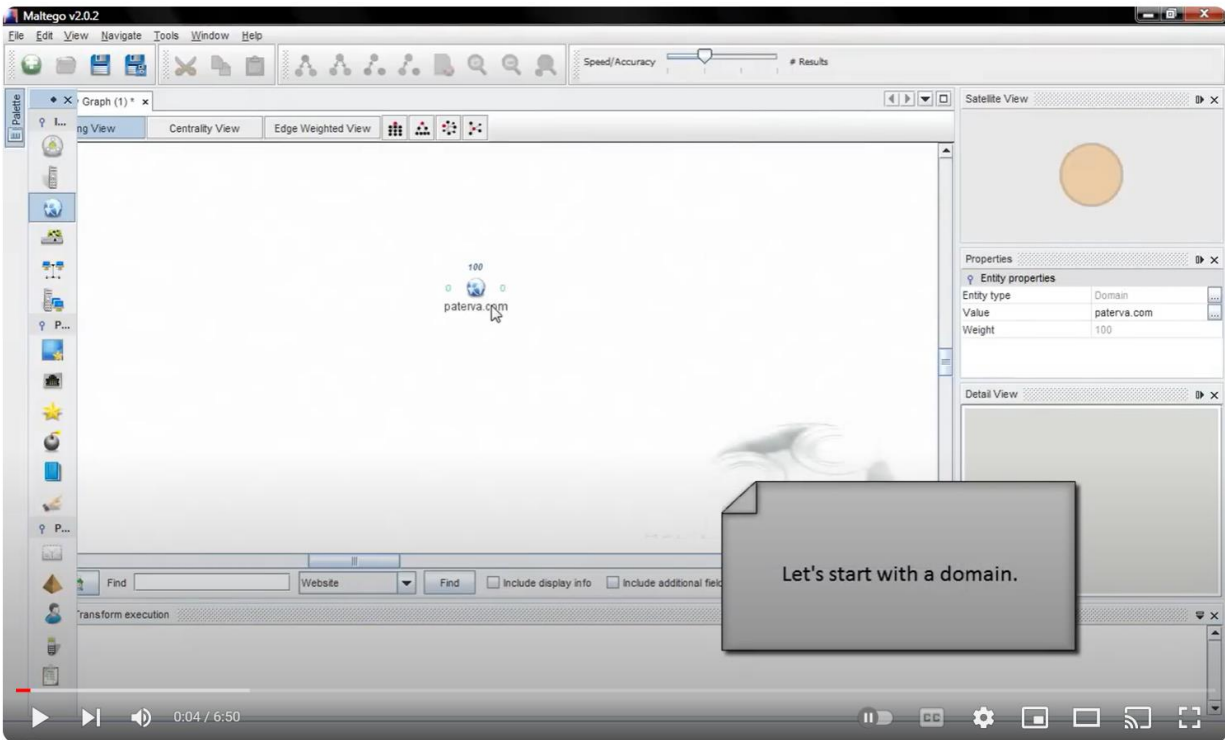
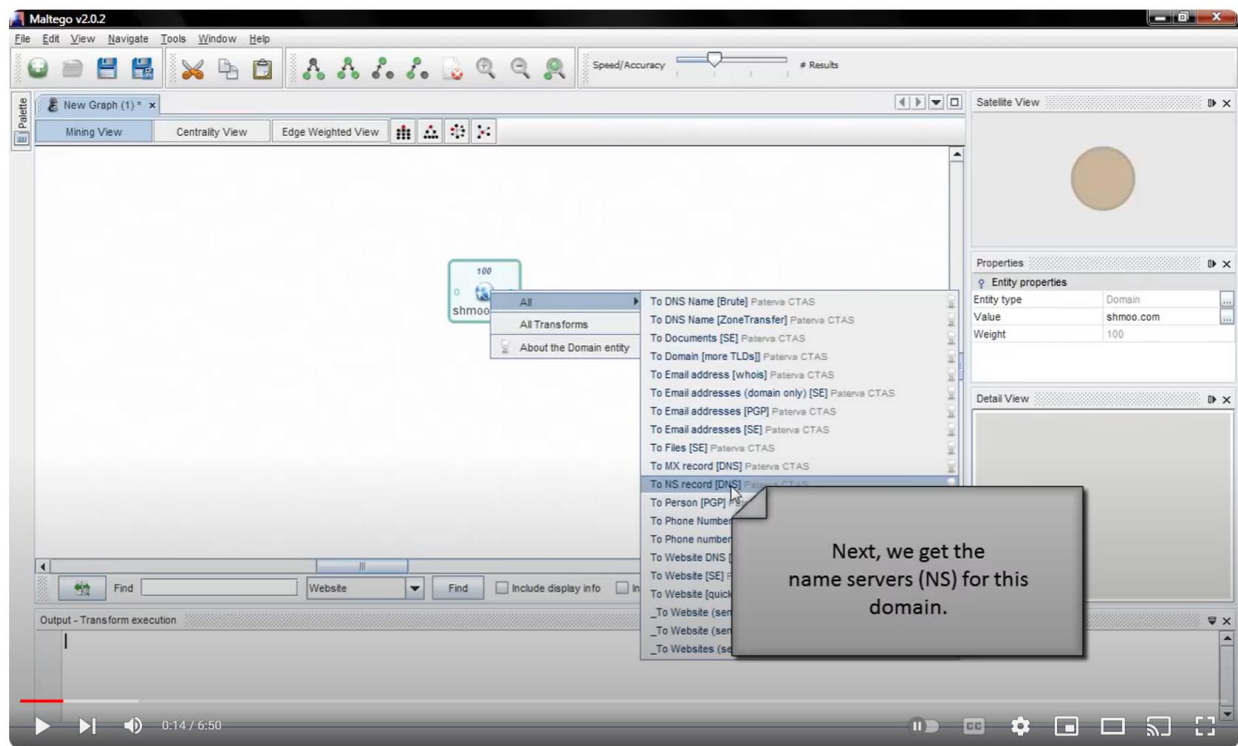








Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Let's see what other domains use these name servers.

shmoos.com

krusty.shmoos.com

archimedes.shmoos.com

All To Domains [DNS] Paterva CTAS

All Transforms To Domains [SharedNS] Paterva CTAS

About the NS Record entity To IP Address [DNS] Paterva CTAS

To Netblock [NS4block] Paterva CTAS

Properties

Entity properties

Entity type NSRecord

Value archimedes.shmoos.com

Weight 100

Detail View

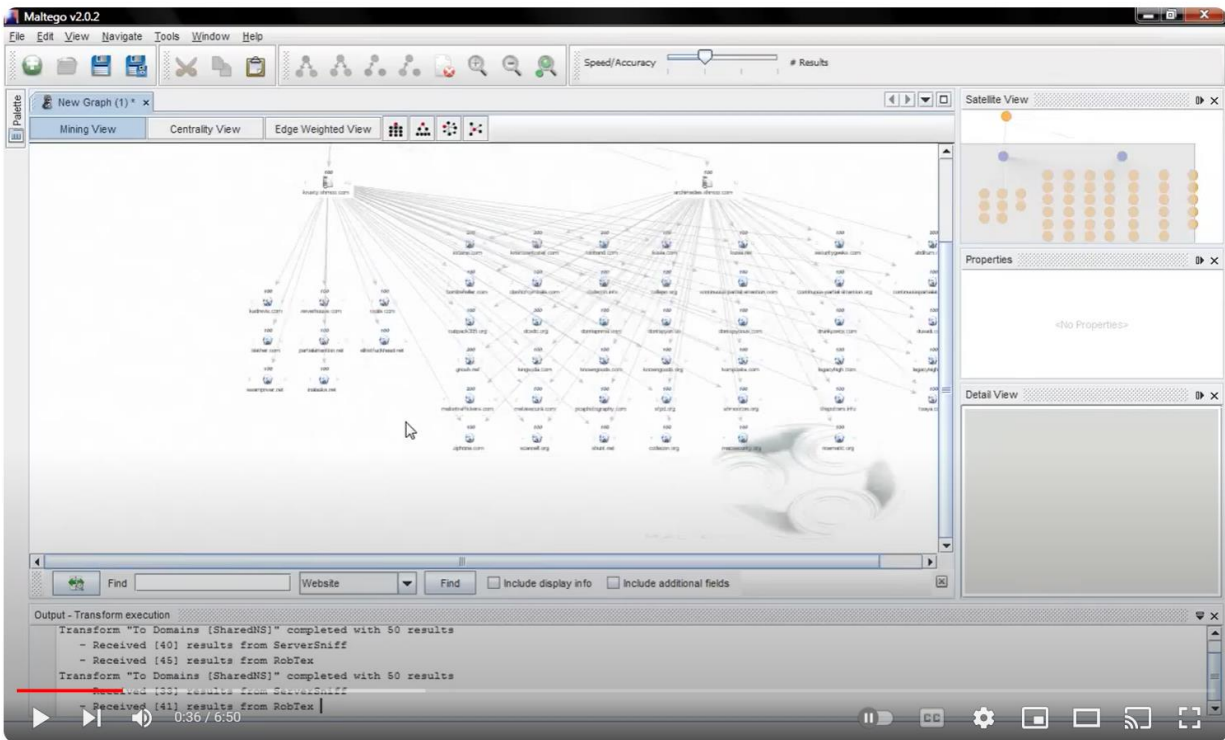
GENERATION INFORMATION

Result	Source	Gen. by
archimedes.shmoos.com (NSRecord)	shmoos.com (Domain)	To NS record [DNS]
		2009-3-23 15:36

Output - Transform execution

Transform "To NS record [DNS]" completed with 2 results

0:19 / 6:50



Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Properties

Entity properties

Entity type	Domain
Value	<Different Values>
Weight	<Different Values>

Detail View

- kusia.net
- legacyhigh.com
- legacyhigh.org
- macsecrity.org
- melontraffickers.com
- metasecure.com
- noematic.org
- pcaphotography.com
- securitygeeks.com
- sfpd.org
- shmoocon.org
- tanhand.com
- thepotters.info
- tsaya.com

When you select multiple nodes they appears as a text list on the right.

Find Website Find Include display info

Output - Transform execution

```
Transform "To Domains (SharedNS)" completed with 50 results
- Received [40] results from ServerSniff
- Received [45] results from RobTex
Transform "To Domains (SharedNS)" completed with 50 results
- Received [33] results from ServerSniff
- Received [41] results from RobTex
```

04:11 / 6:50

Maltego v2.0.2

File Edit View Navigate Tools Window Help

New Graph (1) x

Mining View Centrality View Edge Weighted View

Properties

Entity properties

Entity type Domain

Value tsaya.com

Weight 200

Detail View

GENERATION INFORMATION

Result	tsaya.com	(Domain)
Source	archimedes.shmoo.com	(NSRecord)
Gen. by	To Domains (SharedNS)	2009-3-23 15:36

GENERATION INFORMATION

Result	tsaya.com	(Domain)
--------	-----------	----------

Output - Transform

Received [40] results from Serversniff

Received [45] results from RobTex

Transform "To Domains (SharedNS)" completed with 50 results

Received [40] results from Serversniff

Received [41] results from RobTex

0:55/16:50

We don't know if all these domains are related.

We'll get the email address(es) for each domain from the whois database.

To DNS Name [Brute] Paterva CTAS

To DNS Name [ZoneTransfer] Paterva CTAS

To Documents [SE] Paterva CTAS

To Domain [more TLDs] Paterva CTAS

To Email address [whois] Paterva CTAS

To Email addresses [domain only] [SE] Paterva CTAS

To Email addresses [PGP] Paterva CTAS

To Email addresses [SE] Paterva CTAS

To Files [SE] Paterva CTAS

To MX record [DNS] Paterva CTAS

To NS record [DNS] Paterva CTAS

To Person [POP] Paterva CTAS

To Phone Numbers [SE] Paterva CTAS

To Phone numbers [whois] Paterva CTAS

To Website DNS [SE] Paterva CTAS

To Website [SE] Paterva CTAS

To Website [quick lookup] Paterva CTAS

_To Website (sensitive data -anywhere) Paterva BUNNY

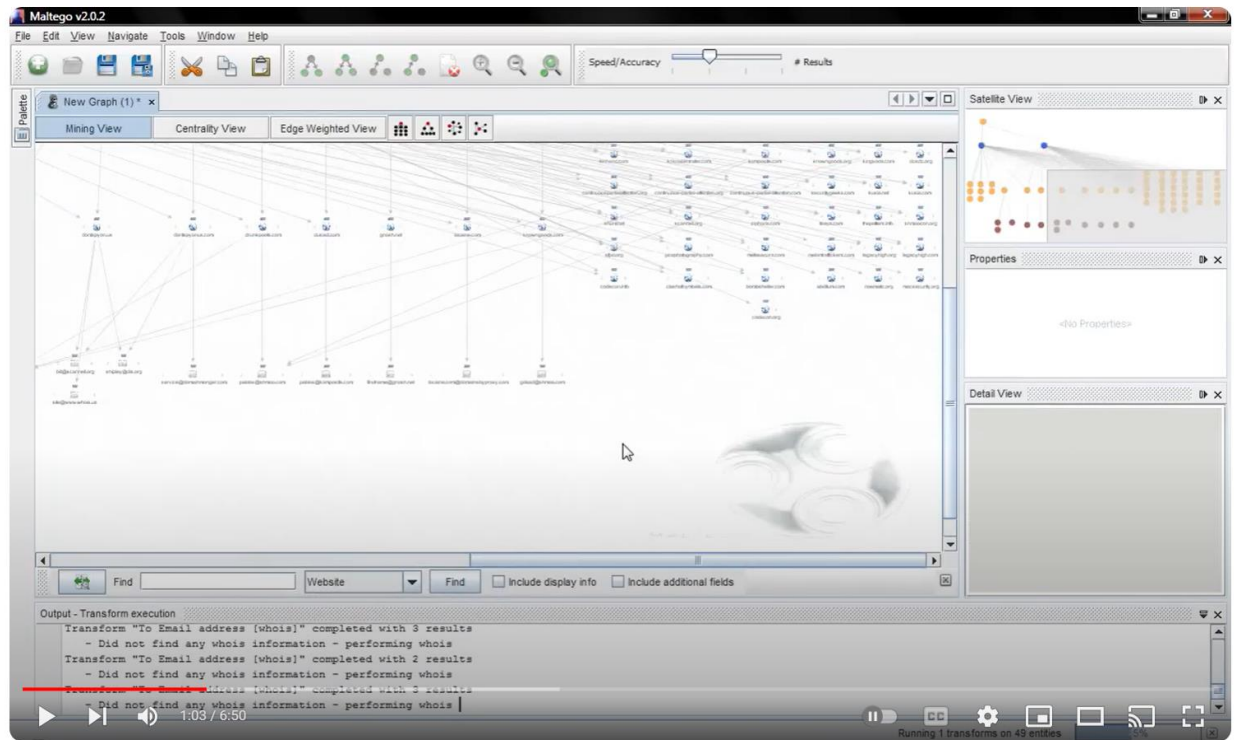
_To Website (sensitive data -domain only) Paterva BUNNY

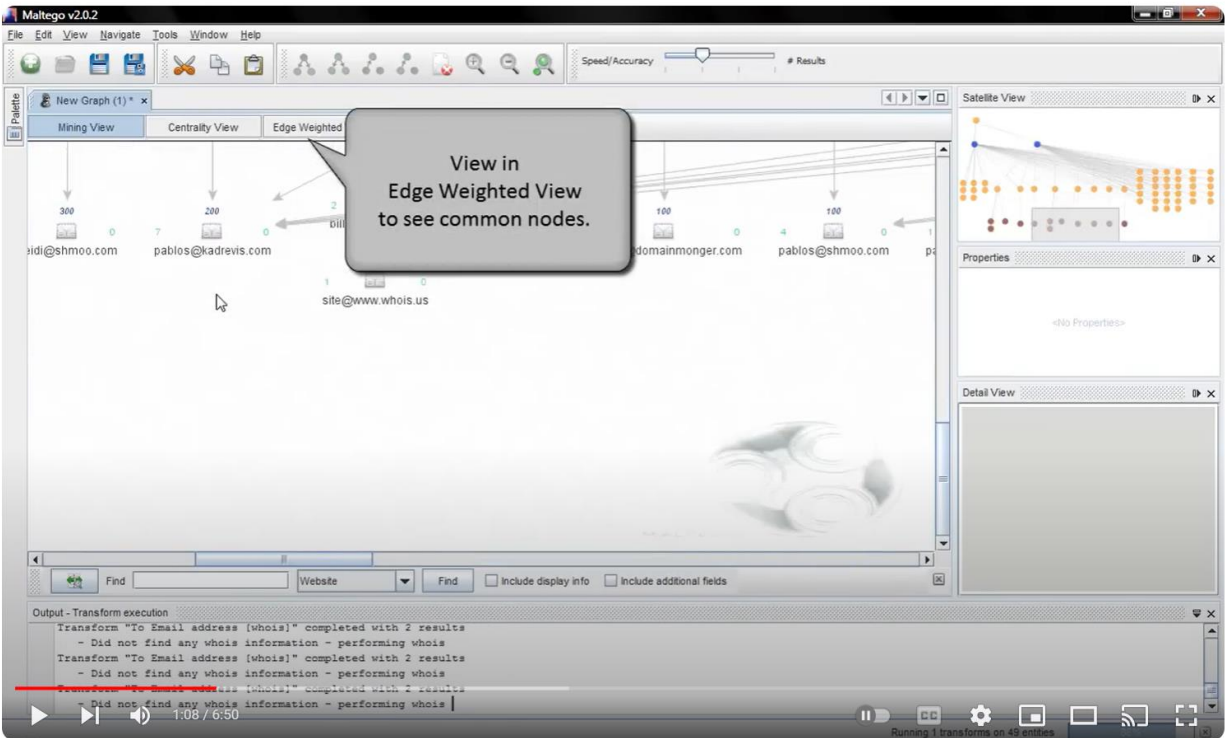
_To Websites (searching in domain with SE) Paterva BUNNY

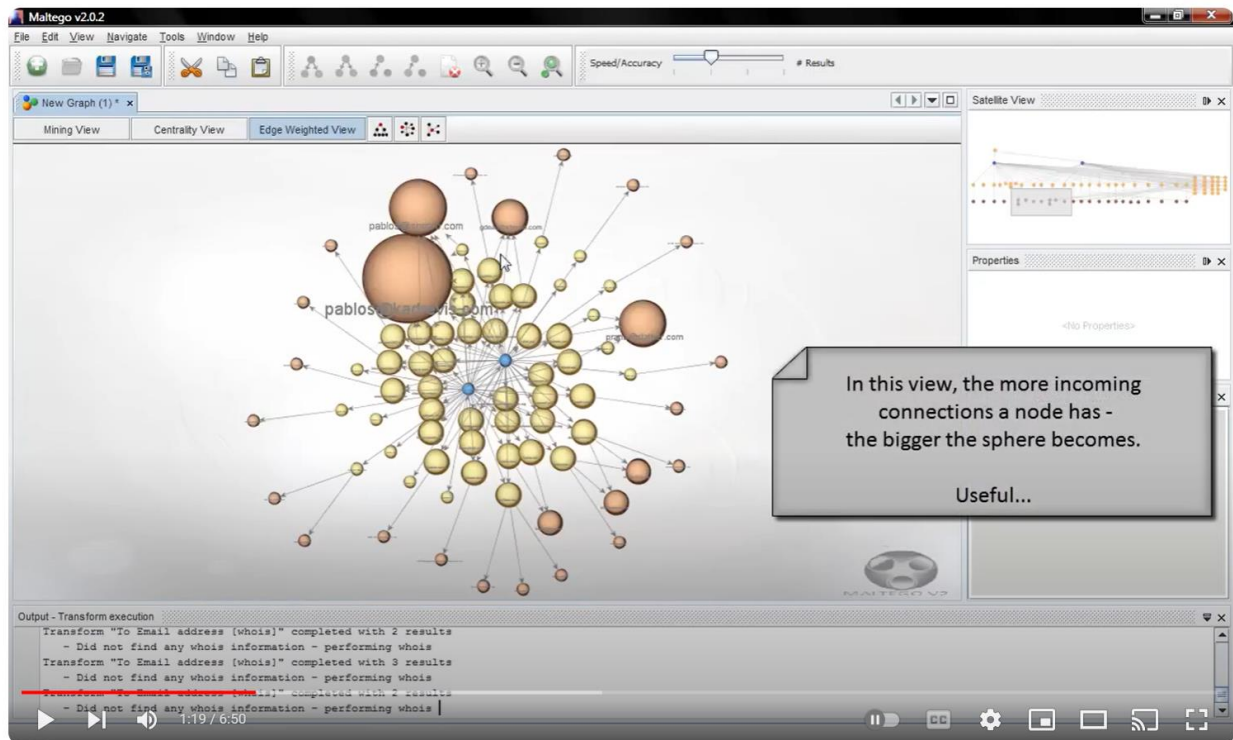
All Transforms

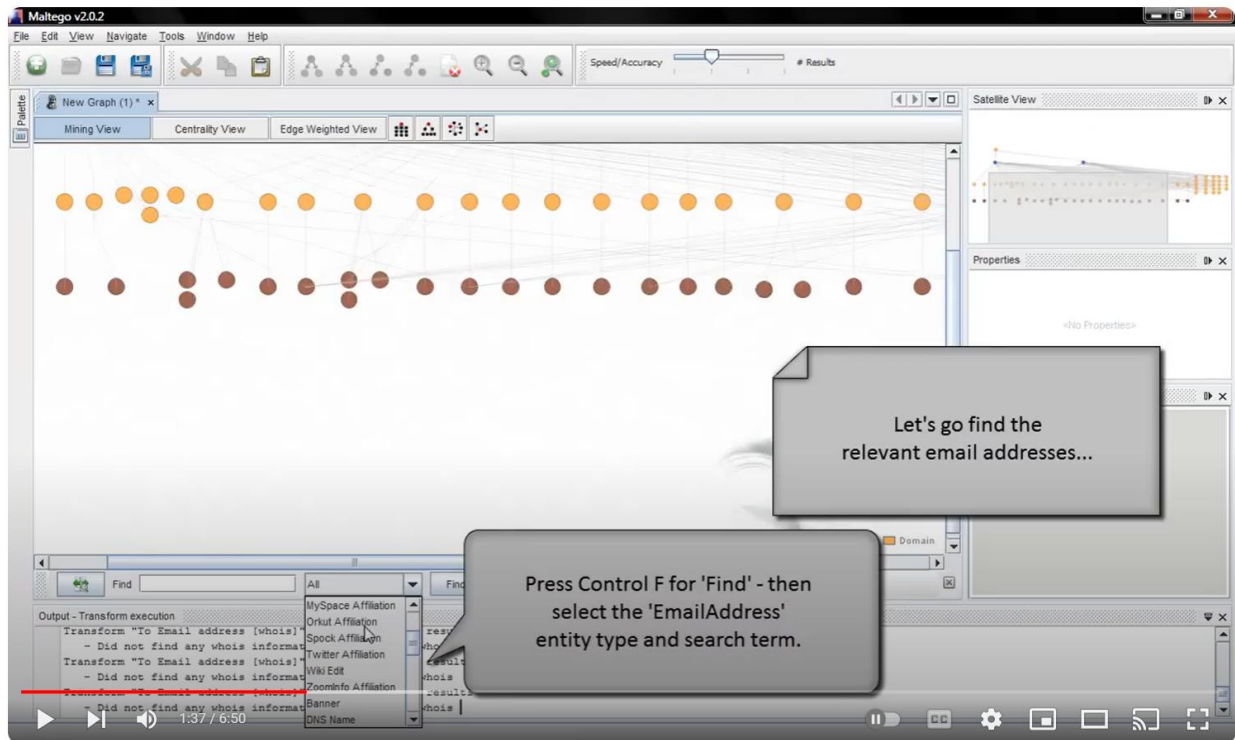
About the Domain entity

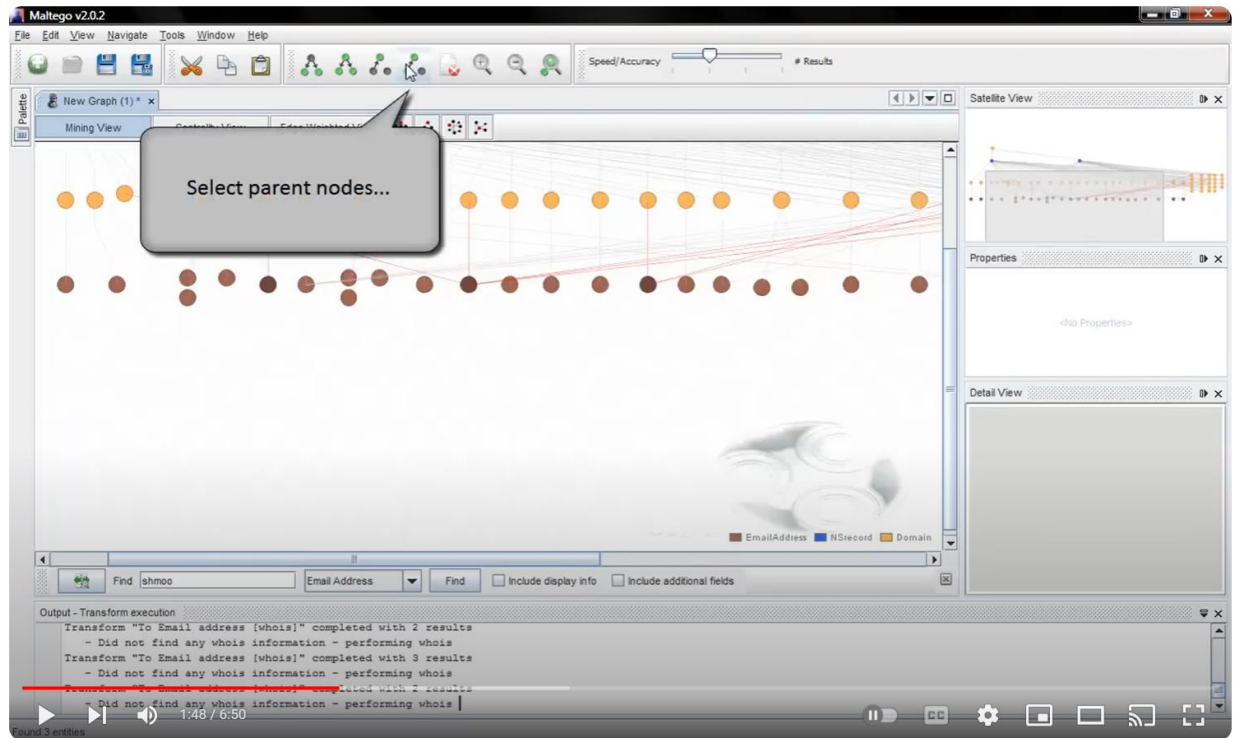
Include display info ☐ Include additional fields

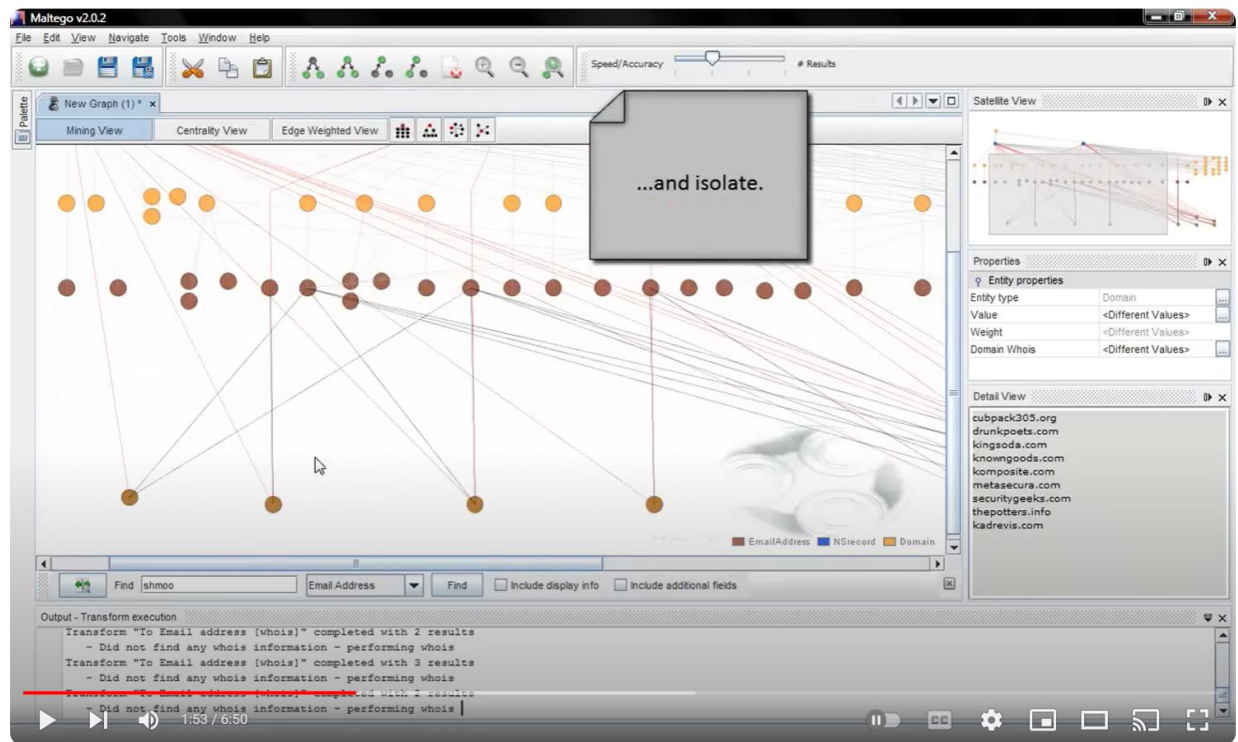


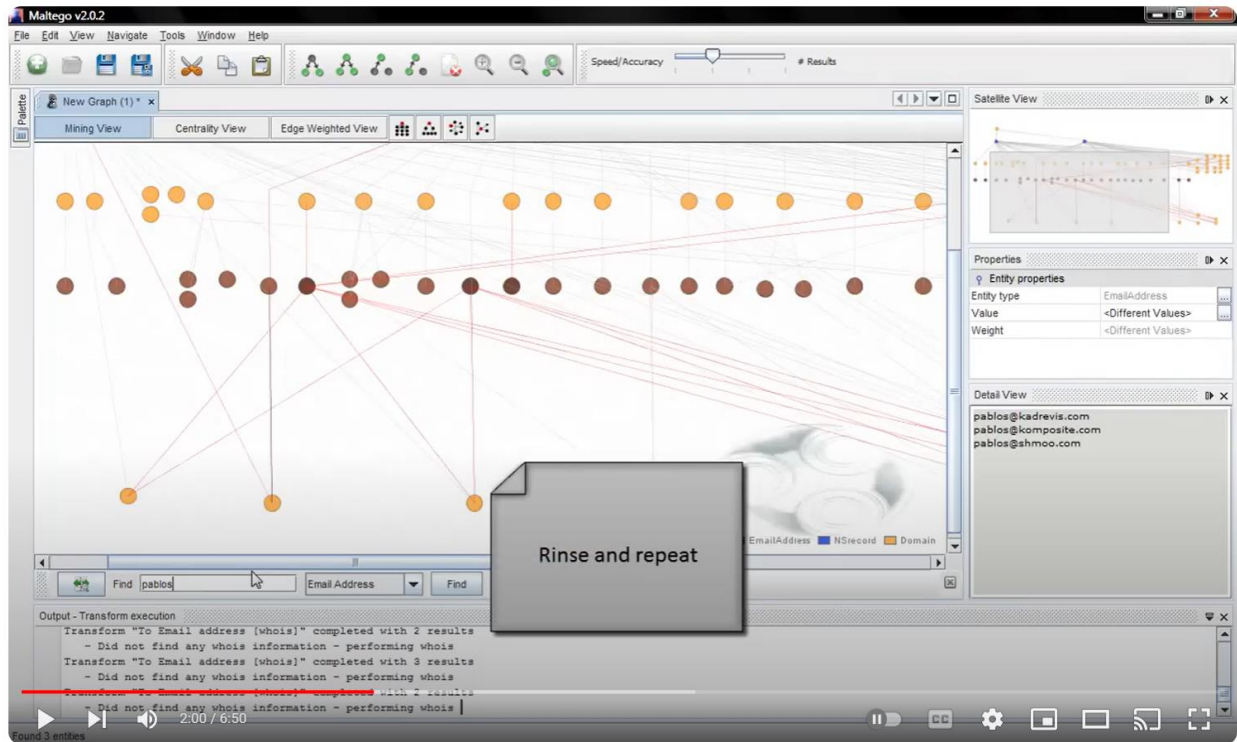


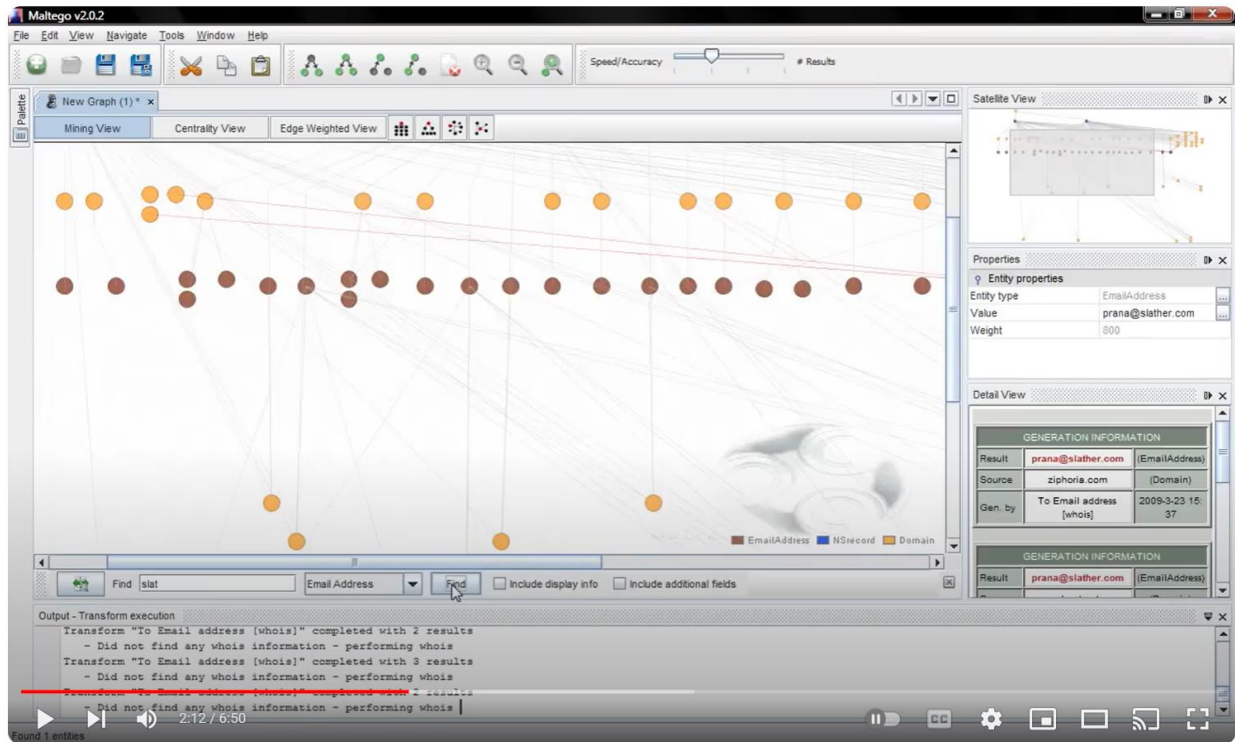


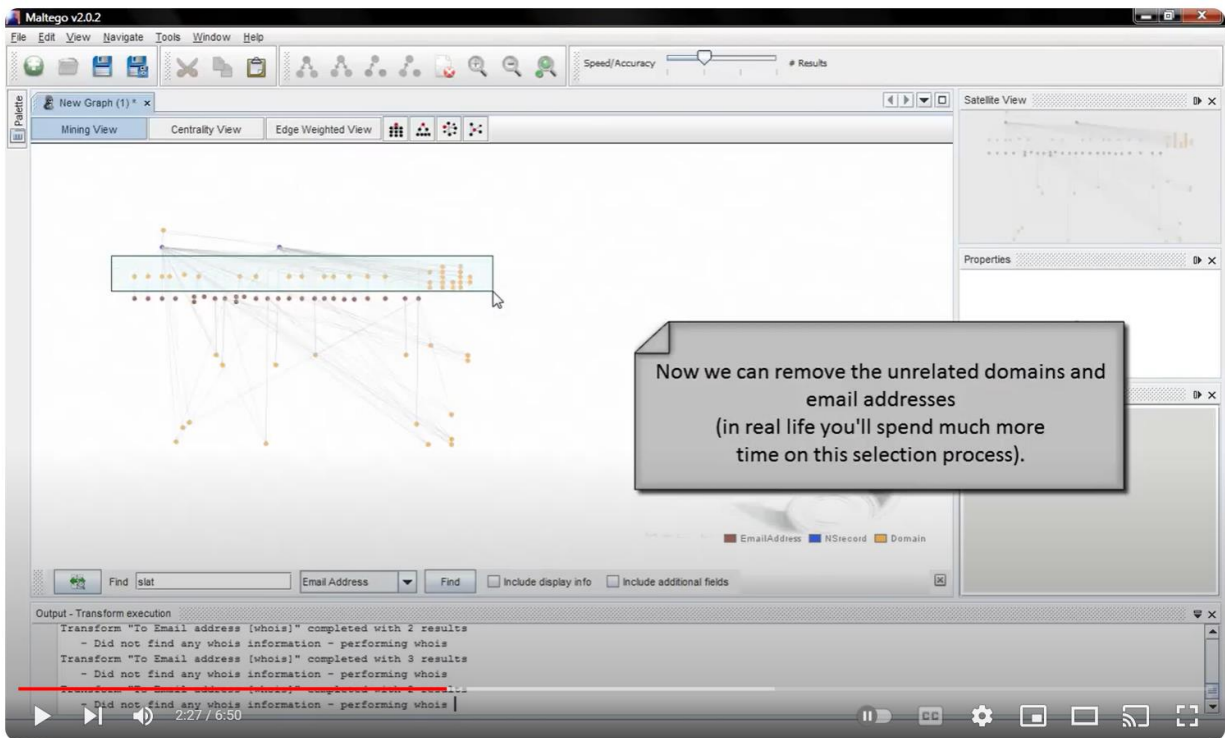












Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Select child nodes - remove them too!

Properties

Entity properties

Entity type	Domain
Value	<Different Values>
Weight	<Different Values>

Detail View

legacyhigh.org
macsecurity.org
melontraffickers.com
noematic.org
pcaphotography.com
sfpd.org
shmoocon.org
tenhand.com
scannell.org
swampriver.net
elbistfuckhead.net
partialattention.net
tsolis.com
neverhouse.com

Find slat Email Address Find Include display info Include additional fields

Output - Transform execution

Transform "To Email address [whois]" completed with 2 results
- Did not find any whois information - performing whois
Transform "To Email address [whois]" completed with 3 results
- Did not find any whois information - performing whois
~~Transform "To Email address [whois]" completed with 2 results~~
~~- Did not find any whois information - performing whois~~

2:32 / 6:50

Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Properties

Detail View

GENERATION INFORMATION

Result	Source	Gen. by
customerservice@networksolutions.com	thepotters info	To Email address [whois]

Output - Transform execution

Transform "To Email address [whois]" completed with 2 results

- Did not find any whois information - performing whois

Transform "To Email address [whois]" completed with 3 results

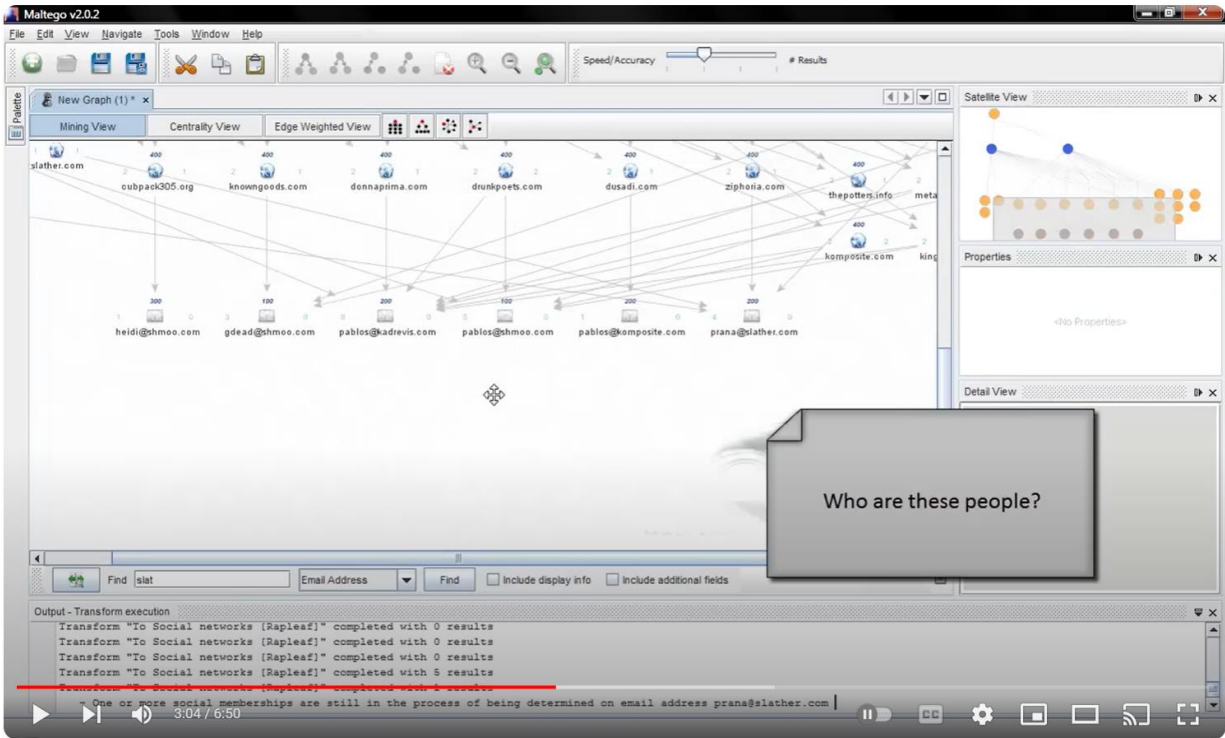
- Did not find any whois information - performing whois

~~Transform "To Email address [whois]" completed with 2 results~~

- Did not find any whois information - performing whois

2:48 / 6:50

We don't need this node (belongs to the ISP).



Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Let's resolve social network membership via Rapleaf...

Output - Transform execution

Transform "To Social networks [Rapleaf]" completed with 0 results

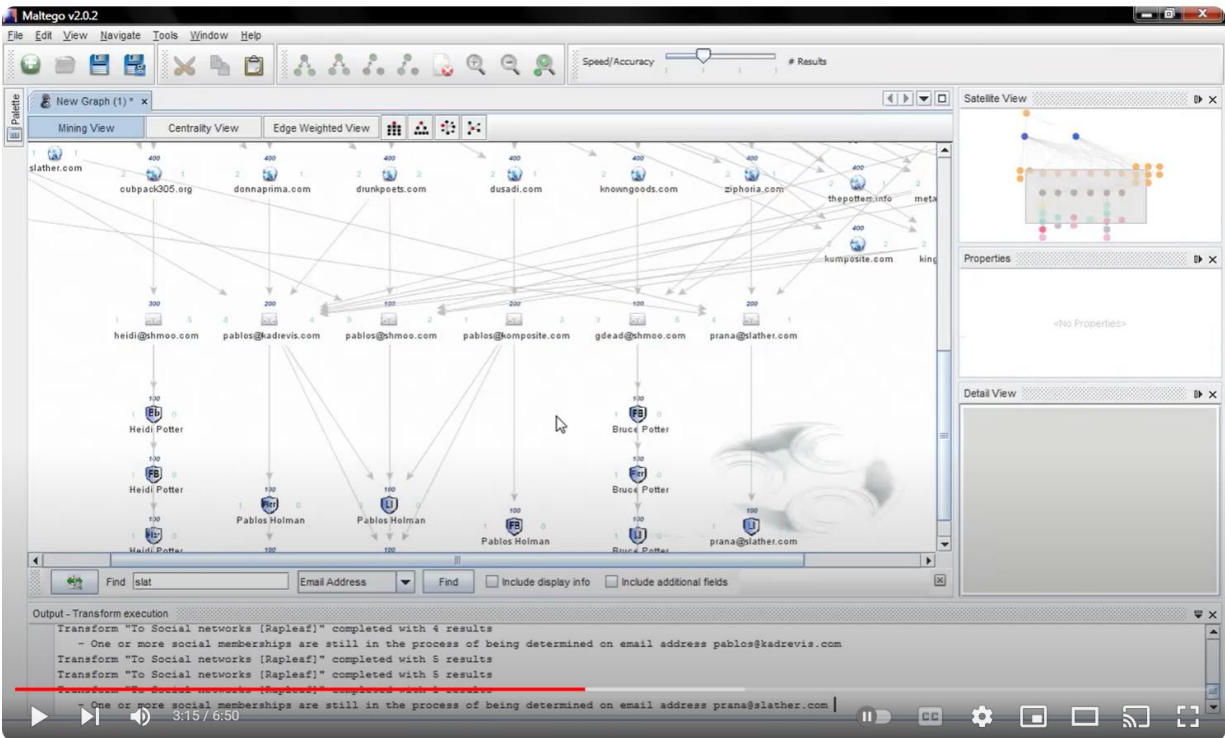
Transform "To Social networks [Rapleaf]" completed with 0 results

Transform "To Social networks [Rapleaf]" completed with 0 results

Transform "To Social networks [Rapleaf]" completed with 5 results

One or more social memberships are still in the process of being determined on email address prana@slather.com

3:10 / 6:50



Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Heidi Potter
Heidi Potter
Heidi Potter
Heidi Potter
Heidi Potter
Heidi Potter
Heidi Potter

Pablos Holman
Pablos Holman
Pablos Holman
Pablos Holman

Bruce Potter
Bruce Potter
Bruce Potter
Bruce Potter
Bruce Potter
Bruce Potter
Bruce Potter

prana@lather.com

Pics or it didn't happen!

Find slat Email Address Find Include display info Include additional fields

Output - Transform execution

Transform "To Social networks [Rapleaf]" completed with 4 results
 - One or more social memberships are still in the process of being determined on email address pablos@kadrevis.com

Transform "To Social networks [Rapleaf]" completed with 5 results

Transform "To Social networks [Rapleaf]" completed with 5 results

~~Transform "To Social networks [Rapleaf]" completed with 4 results~~
 - One or more social memberships are still in the process of being determined on email address prana@lather.com

3:32 / 6:50

Satellite View

Properties

Entity properties

Entity type AffiliationFlickr
 Value Pablos Holman
 Weight 100
 Unique identifier people/pablos06/
 Network (key) Flickr

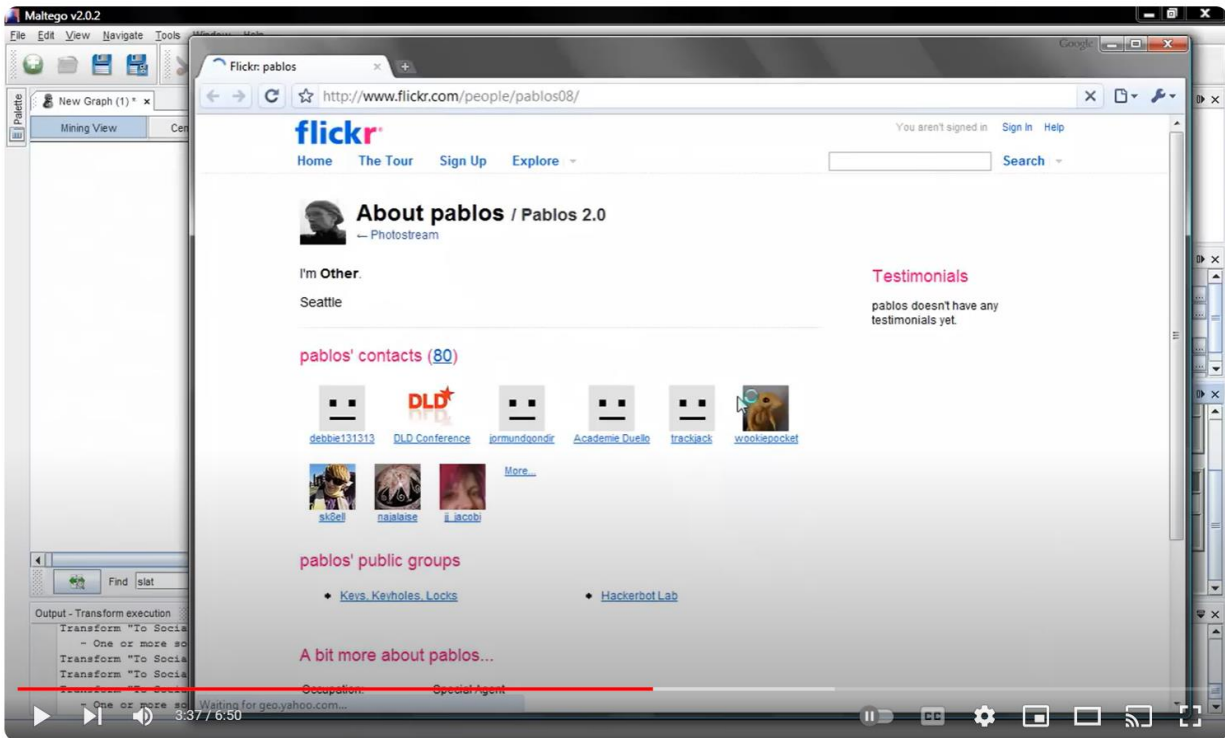
Detail View

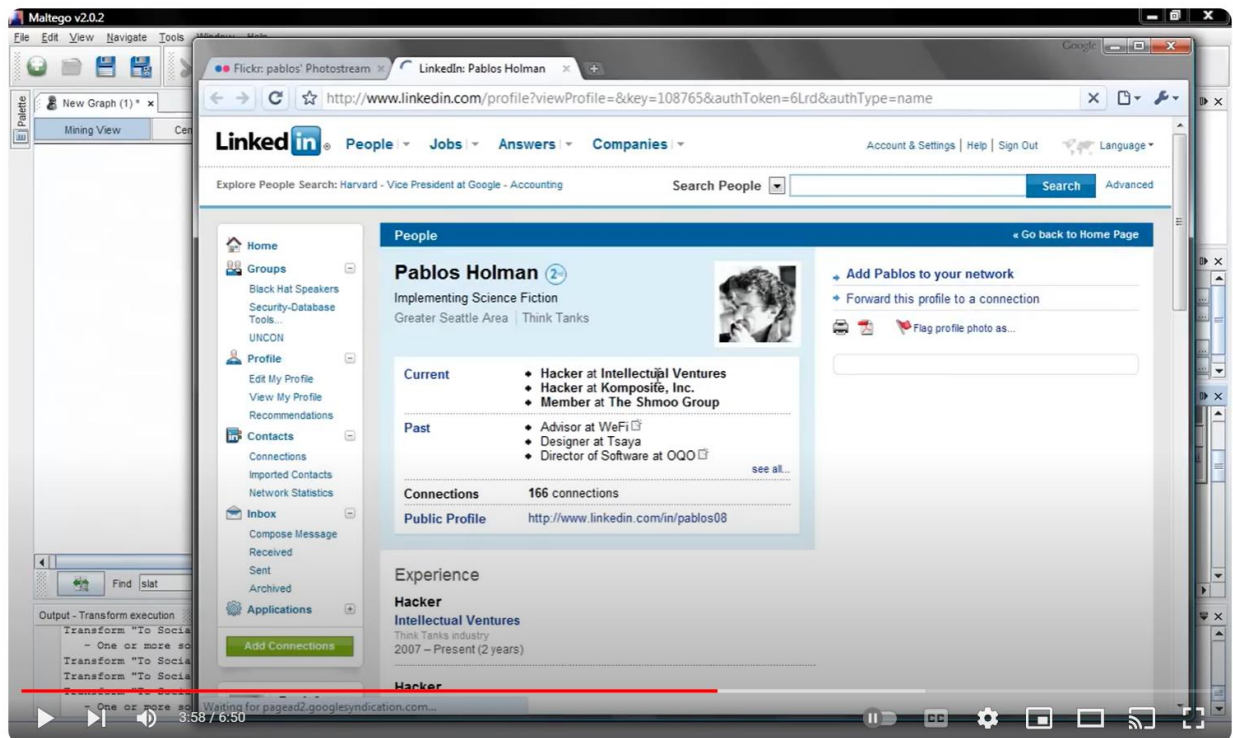
GENERATION INFORMATION

Result	Pablos Holman	(AffiliationFlickr)
Source	pablos@kadrevis.com	(EmailAddress)
Gen. by	To Social networks [Rapleaf]	2009-3-23 15:44

Social network membership: Flickr

UID people/pablos06/





Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) *

Mining View Centrality View Edge Weighted View

heidi@shmoo.com pablos@kadrevis.com pablos@shmoo.com pablos@komposite.com gdead@shmoo.com prana@slather.com

Heidi Potter Pablos Holman Pablos Holman Pablos Holman Bruce Potter prana@slather.com

Properties

Entity properties

Entity type AffiliationLinkedin

Value Bruce Potter

Weight 100

Unique identifier 2253268

Network [key] Linkedin

Detail View

2009-3-23 15:44

network membership: Linkedin

in.com/profile?u=2253268&authToken=GjIV&authType=name

Output - Transform execution

Transform "To Social networks [Rapleaf]" completed with 4 results

- One or more social memberships are still in the process of being determined on email address pablos@kadrevis.com

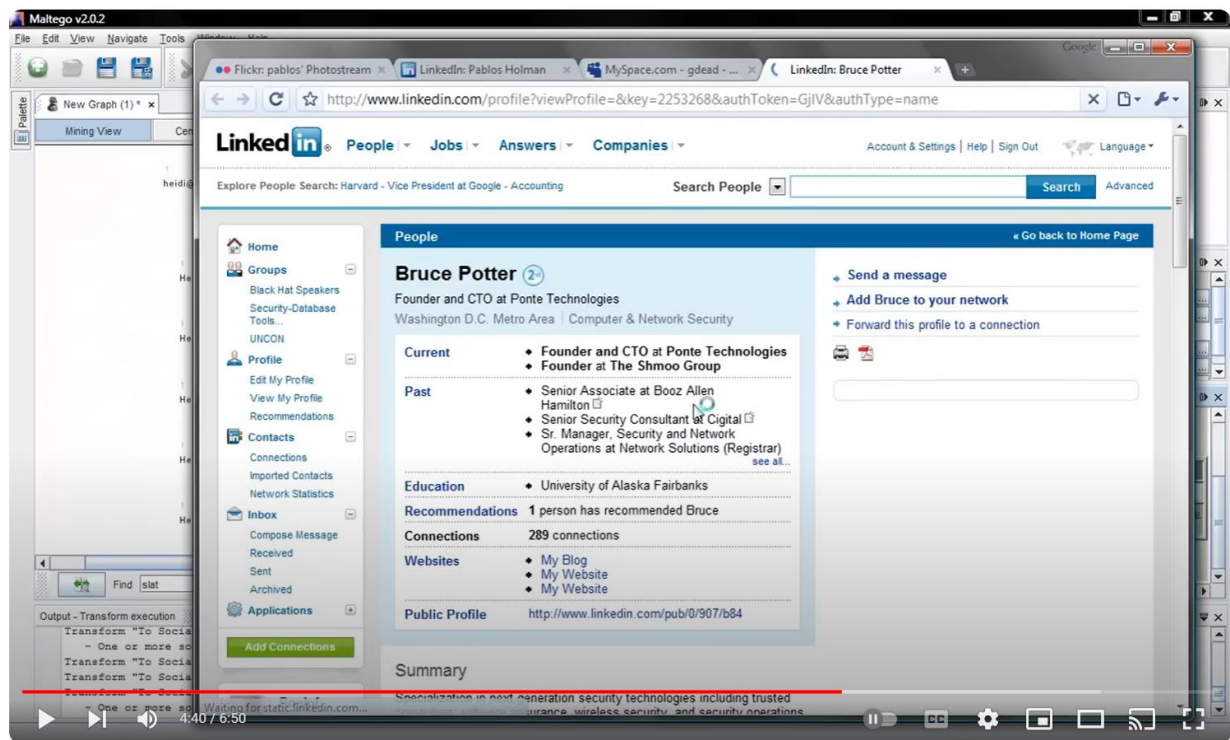
Transform "To Social networks [Rapleaf]" completed with 5 results

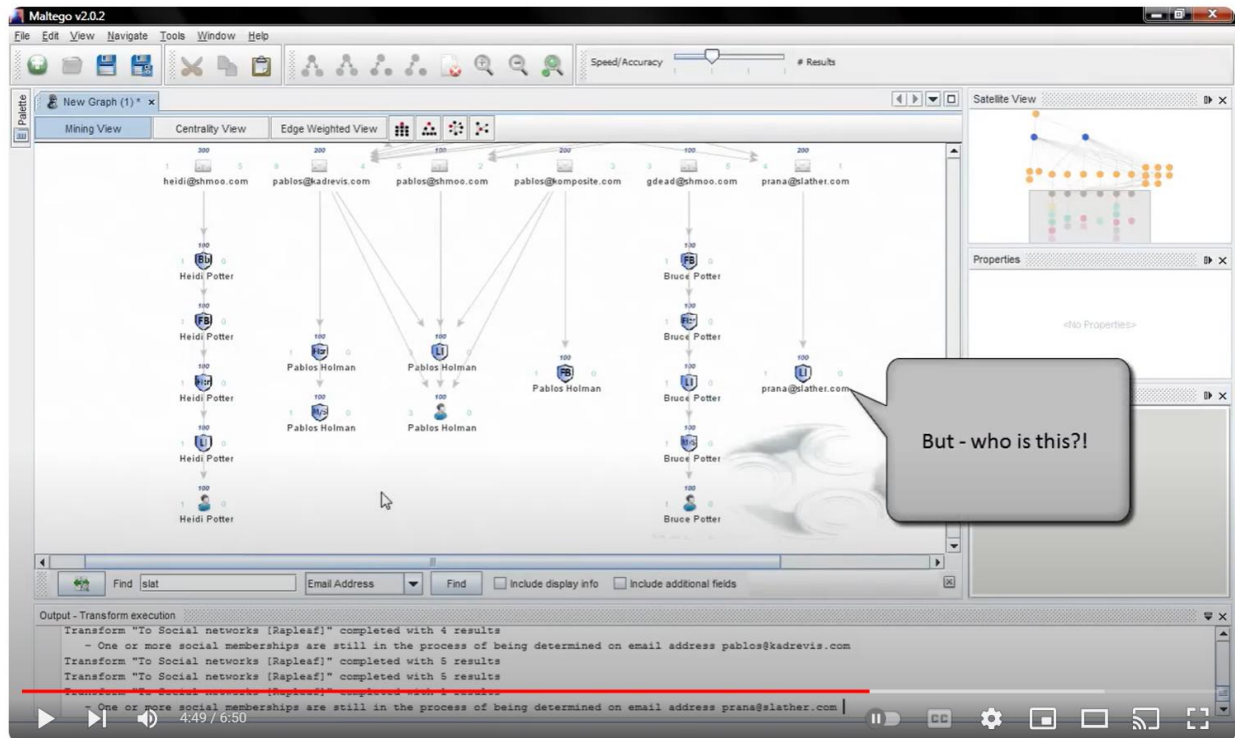
Transform "To Social networks [Rapleaf]" completed with 5 results

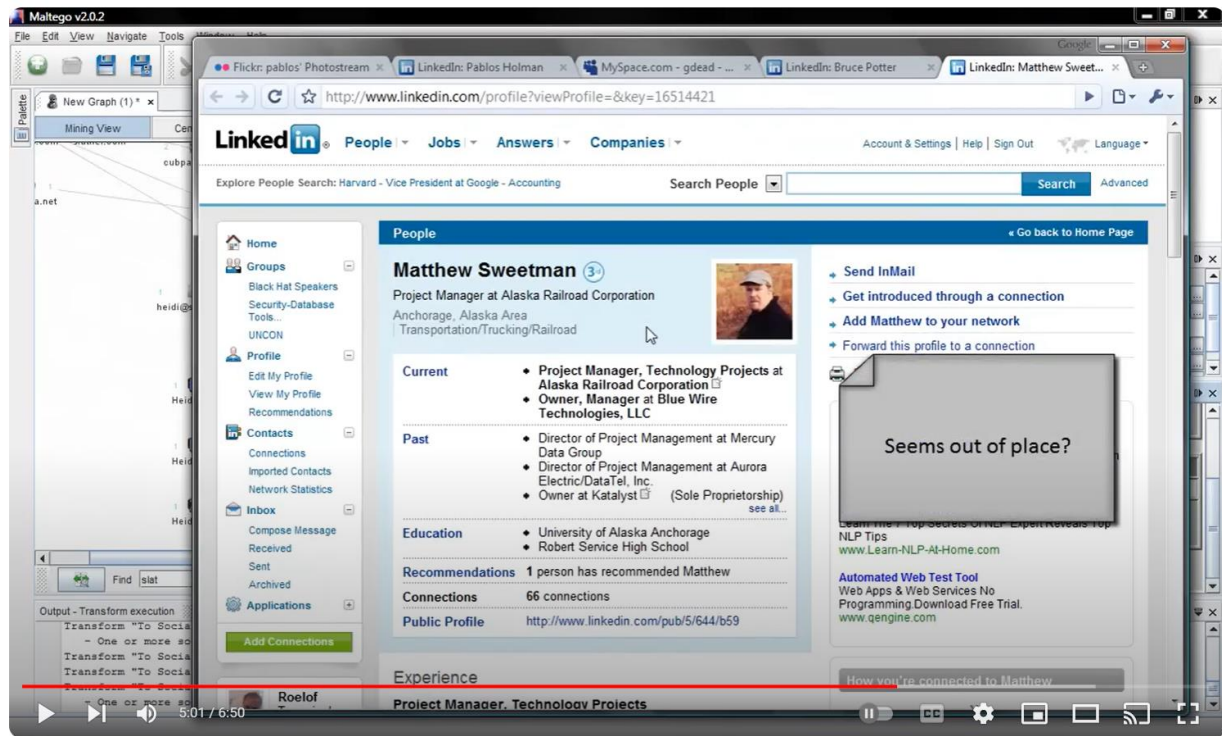
Transform "To Social networks [Rapleaf]" completed with 5 results

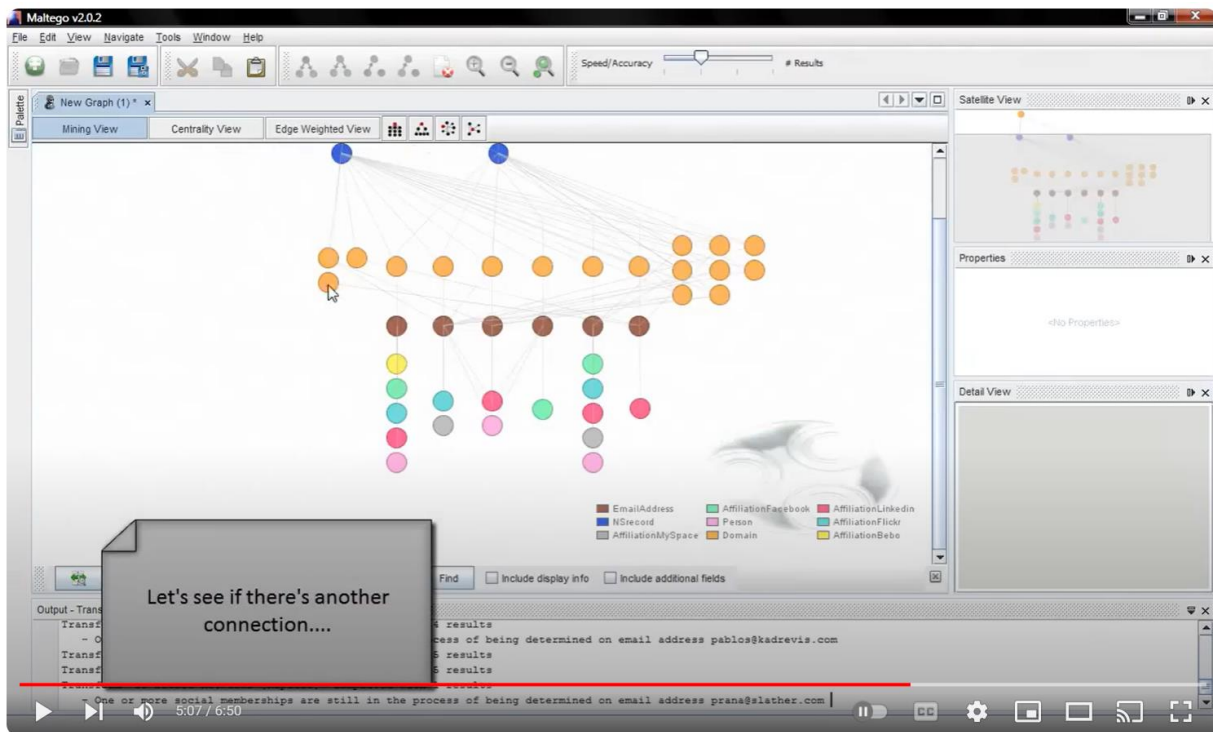
- One or more social memberships are still in the process of being determined on email address prana@slather.com

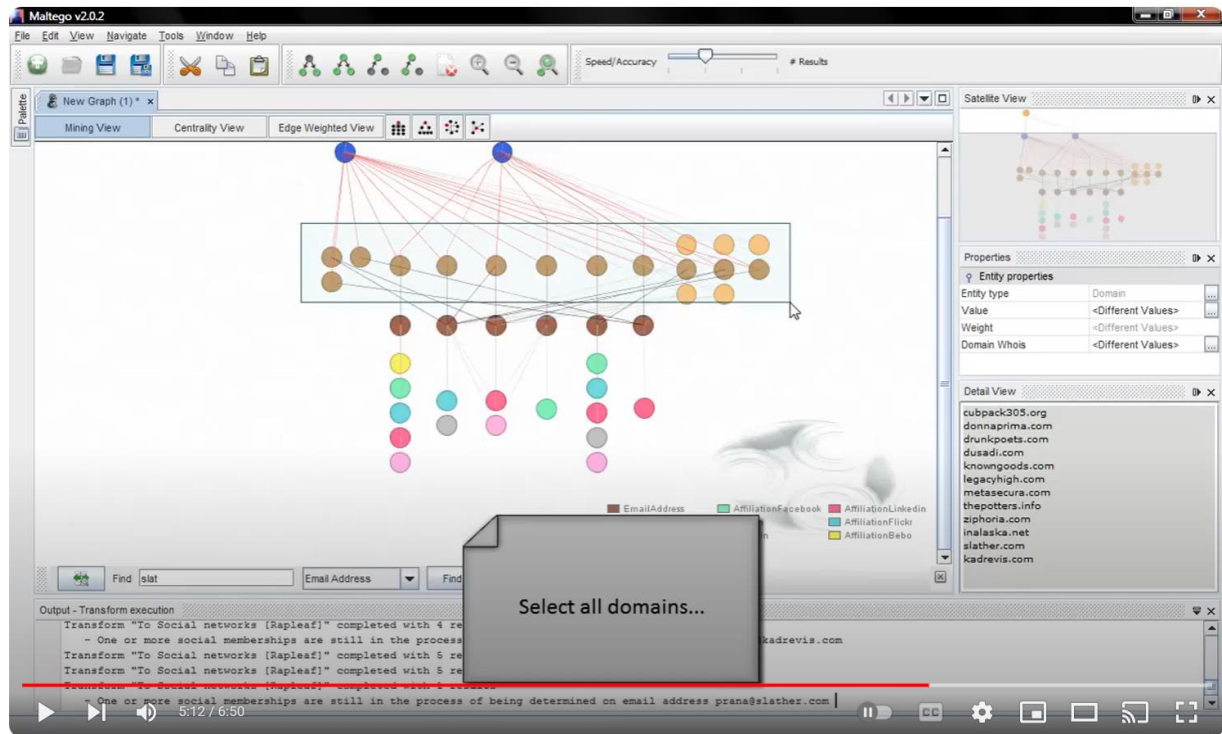
4:37 / 6:50

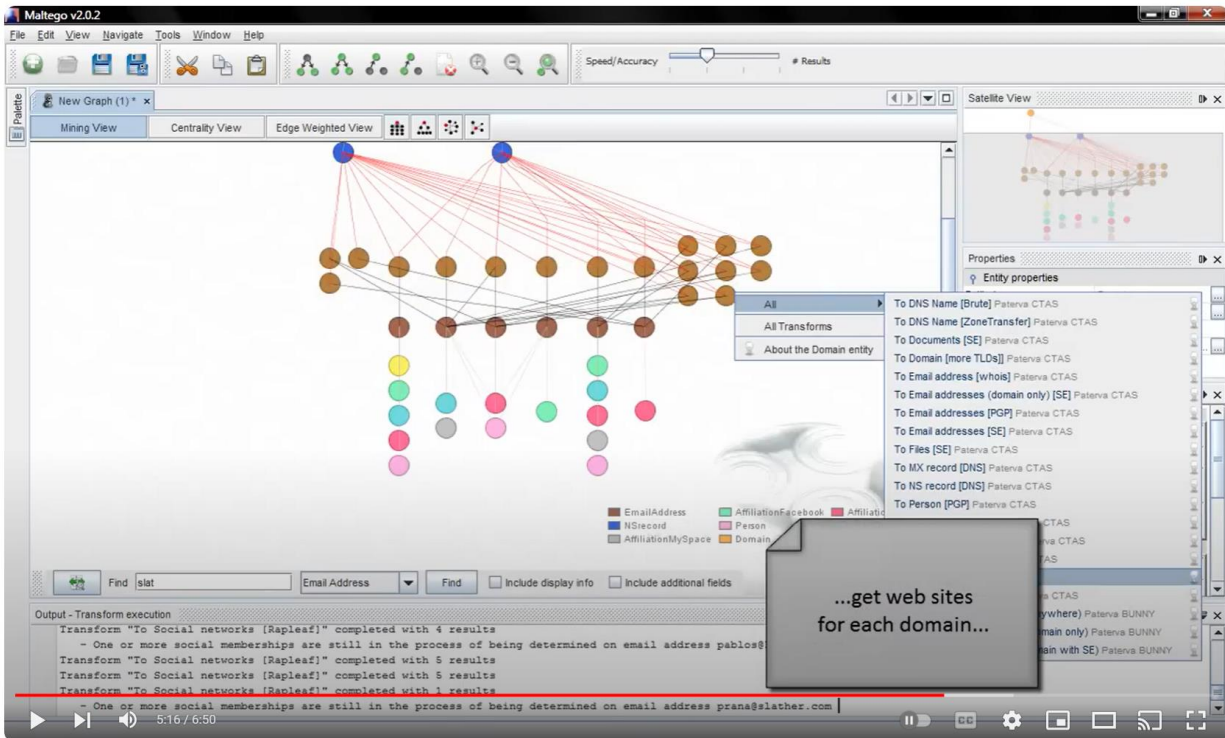


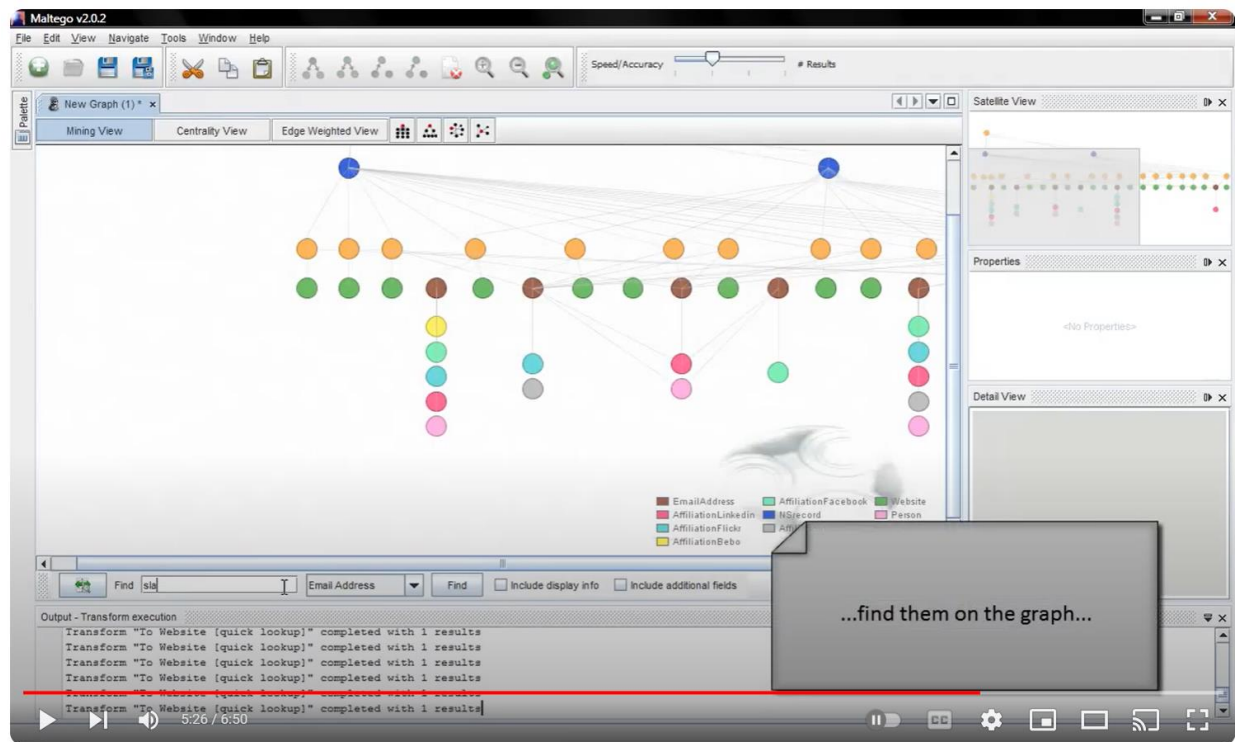












Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) x

Mining View Centrality View Edge Weighted View

Properties

Entity properties

Entity type Website

Value www.inalaska.net

Weight 100

Detail View

GENERATION INFORMATION

Result	www.inalaska.net	(Website)
Source	inalaska.net	(Domain)
Gen. by	To Website [quick lookup]	2009-3-23 15:48

Output - Transform execution

Transform "To Website [quick lookup]" completed with 1 results

Transform "To Website [quick lookup]" completed with 1 results

Transform "To Website [quick lookup]" completed with 1 results

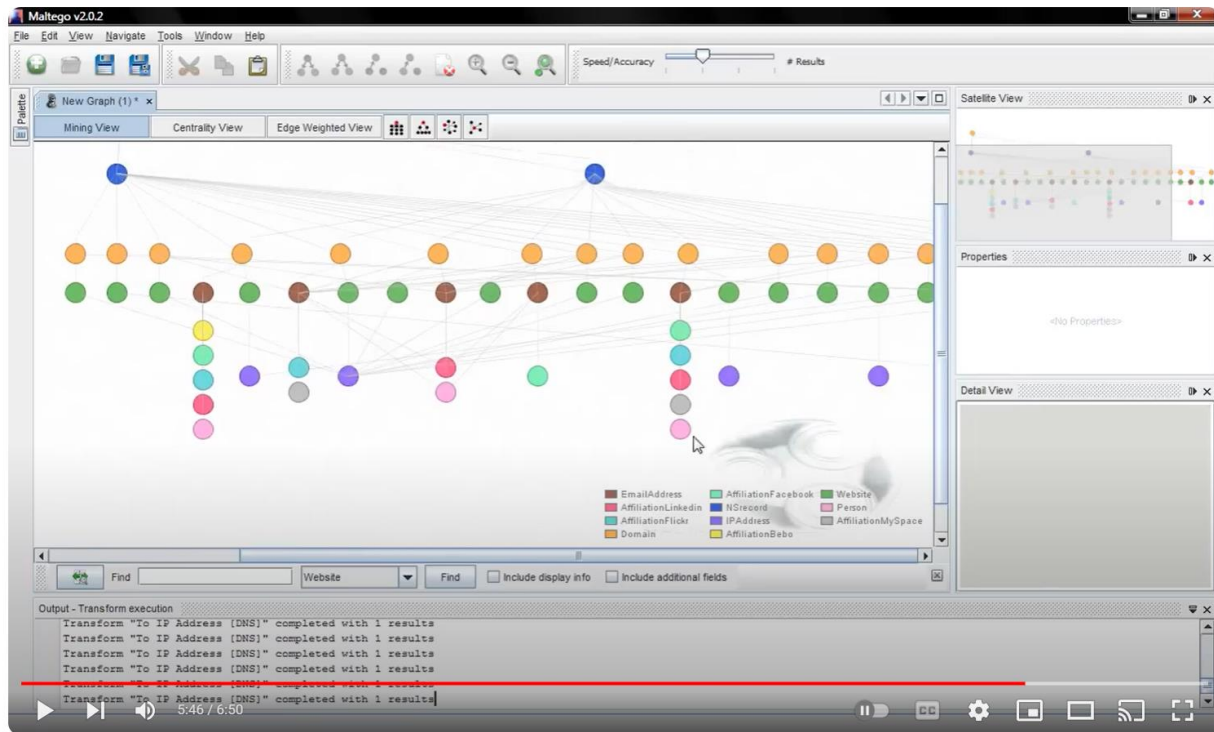
Transform "To Website [quick lookup]" completed with 1 results

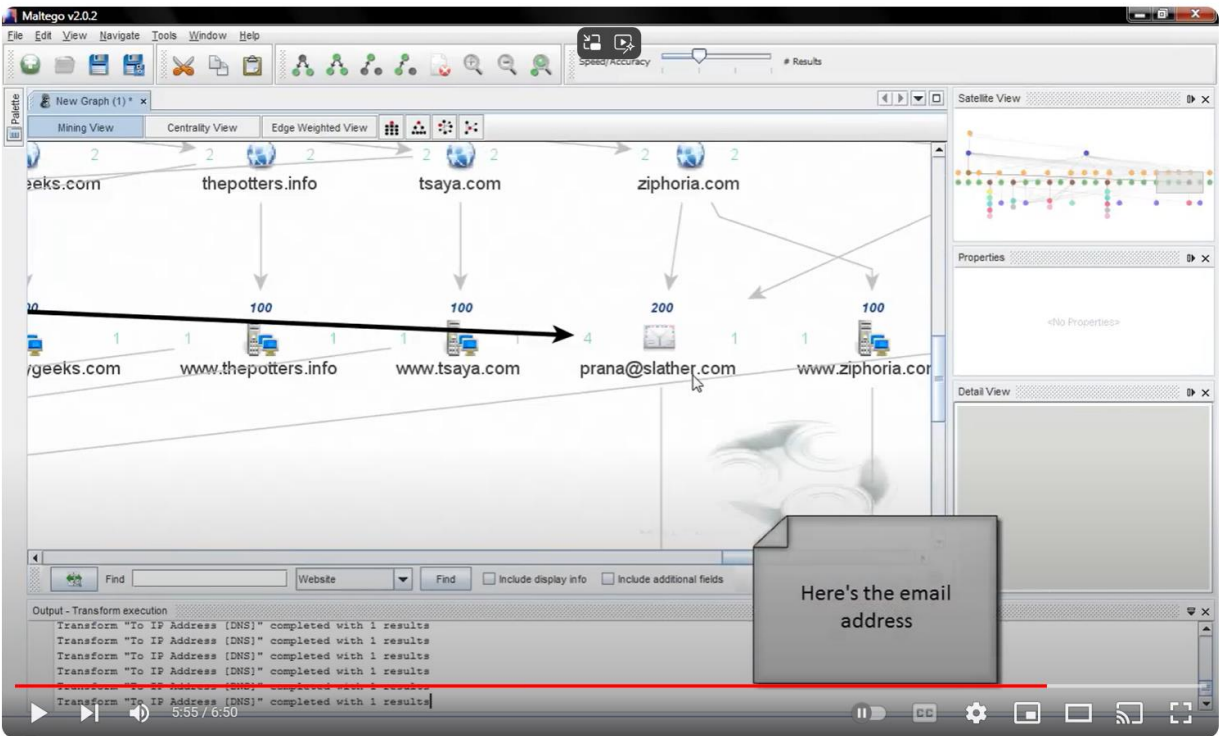
Transform "To Website [quick lookup]" completed with 1 results

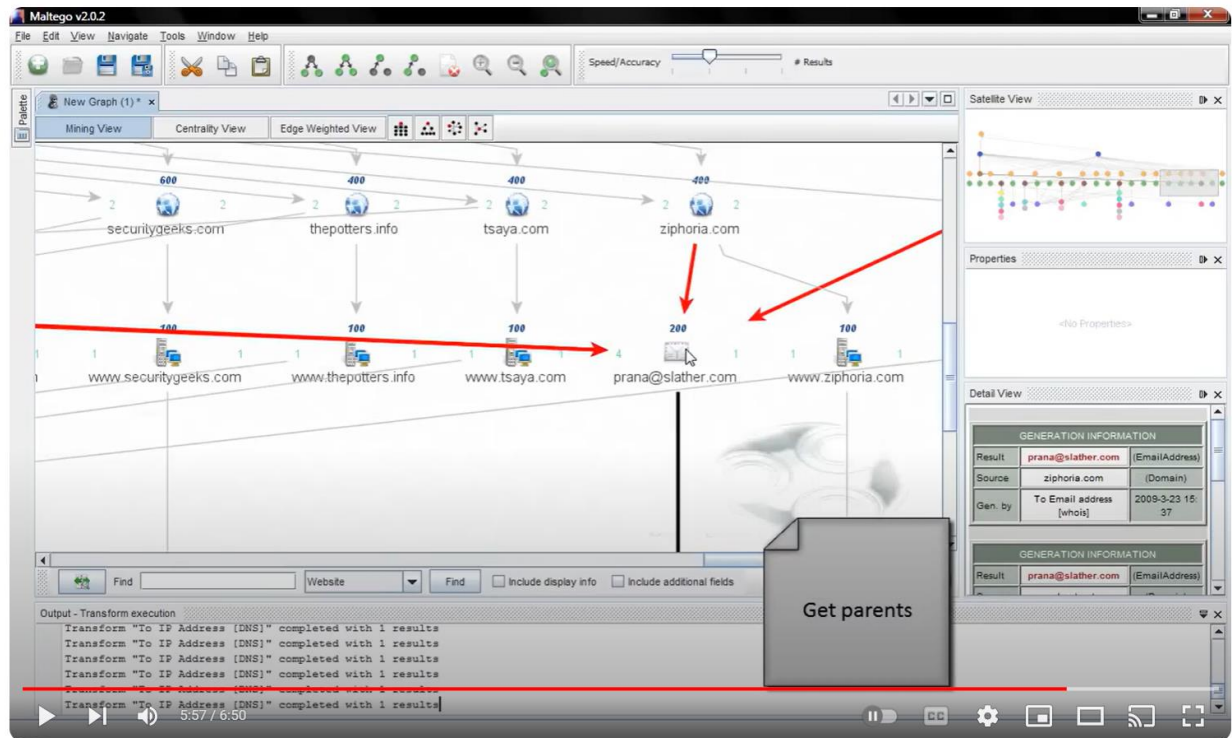
Transform "To Website [quick lookup]" completed with 1 results

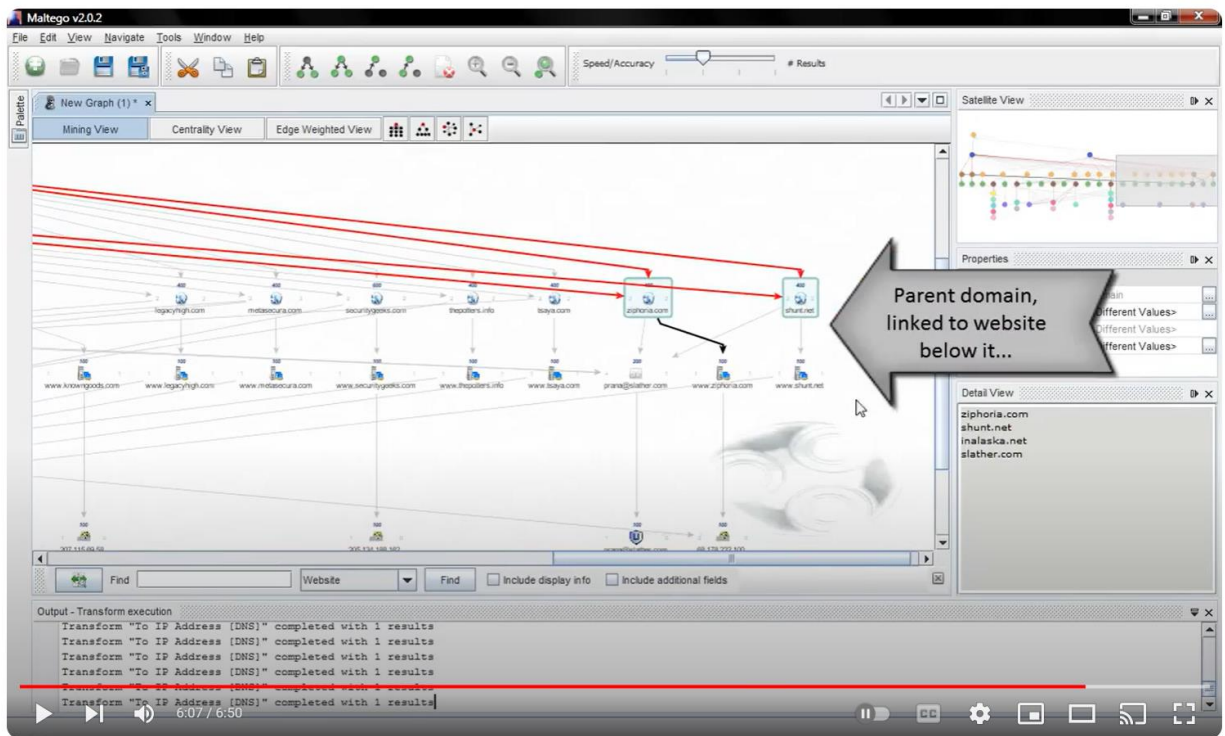
Found 17 entities

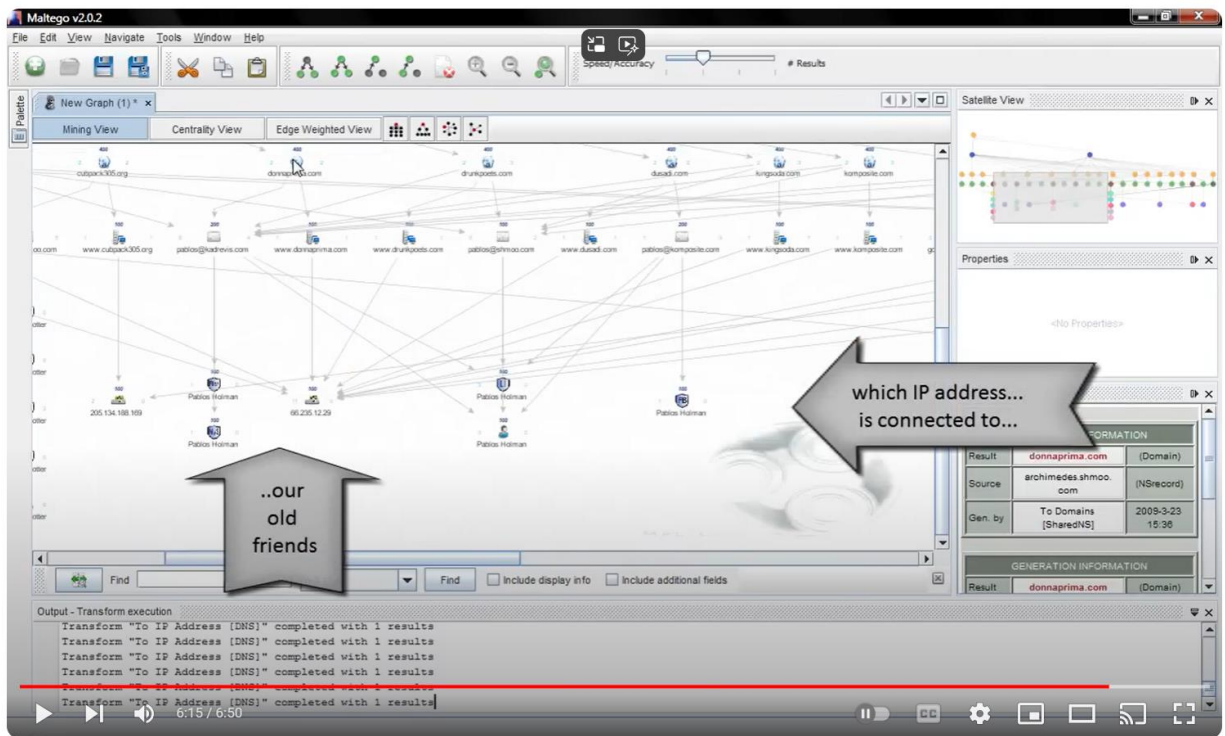
...and resolve their IP addresses.











Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

New Graph (1) *

Mining View Centrality View Edge Weighted View

100 100

r.com www.ziphoria.com www.shu

All

- To Domains [DNS] Paterva CTAS
- To Email Address [Mirror] Paterva CTAS
- To IP Address [DNS] Paterva CTAS
- To Phrase [Blog Tag Technorat] Paterva CTAS
- To URLs [Dun0] Paterva CTAS
- To Website [DNS] Paterva CTAS
- To Website [Incoming links SE] Paterva CTAS
- To Website [Mirror] Paterva CTAS
- To Website [Thumbnail] Paterva CTAS
- _To Webdir (directories found using SE) Paterva PT
- _To Website Title Paterva PT

What does the site look like?

To get an idea let's get the title.

Properties

Entity properties

Entity type Website

Value www.shunt.net

Weight 100

Detail View

GENERATION INFORMATION

Result	www.shunt.net	(Website)
Blog	shunt.net	(Domain)
Can by	To Website [quick lookup]	2008-3-23 15:48

Output - Transform execution

Transform "To IP Address [DNS]" completed with 1 results

Transform "To IP Address [DNS]" completed with 1 results

Transform "To IP Address [DNS]" completed with 1 results

Transform "To IP Address [DNS]" completed with 1 results

Transform "To IP Address [DNS]" completed with 1 results

6:28 / 6:50

