Cork | Sec #6

18:30-19:00 Socialising ☺
19:00-19:30 Password Alternative / SensiPass – Michael Hill
19:30-19:40 Socialising
19:40-20:40 Maltego 101 – Bob McArdle
20:40-??? More Socialising

corksec.robertmcardle.com
Meetup.com/CorkSec

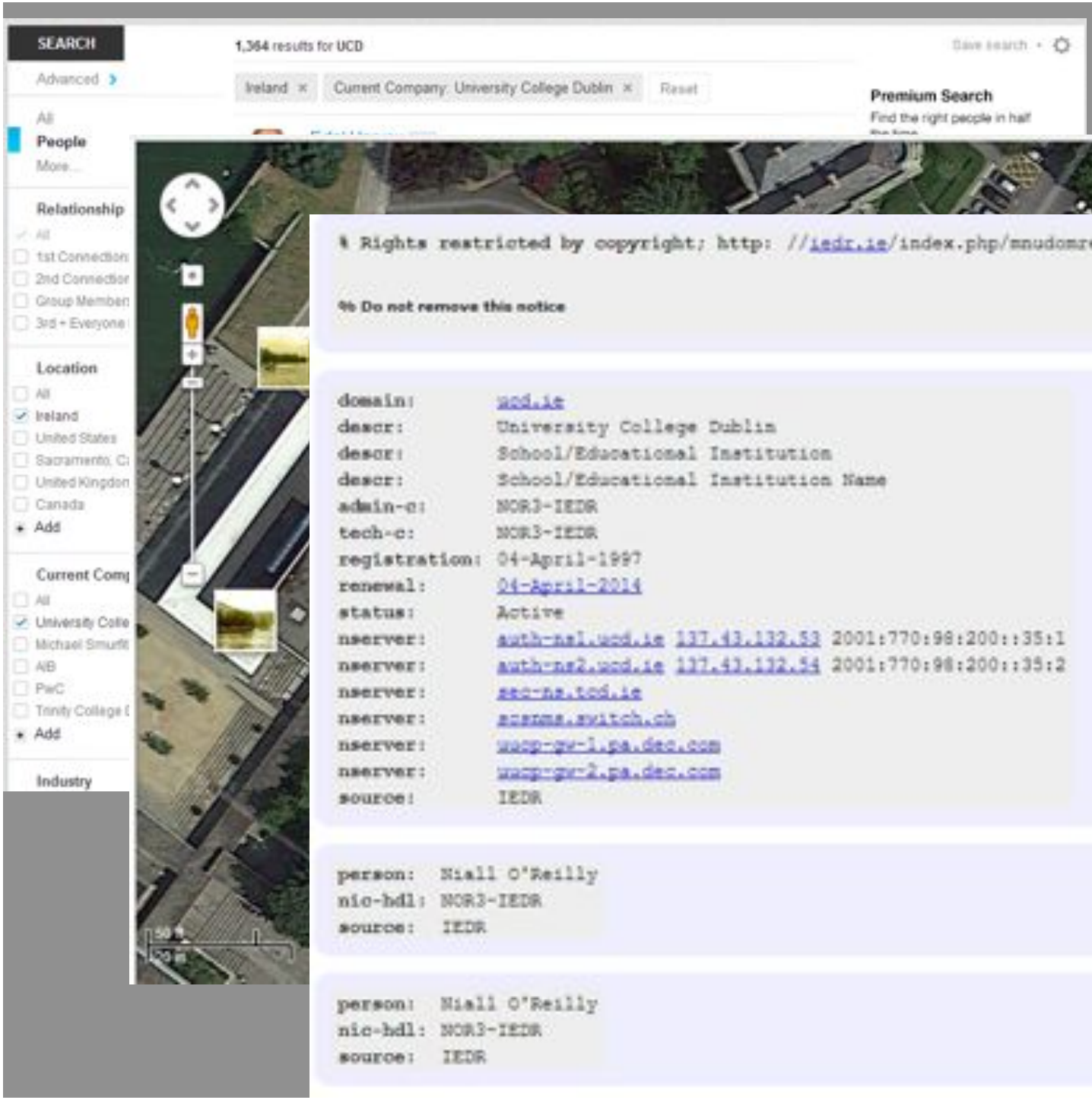
Maltego 101

Bob McArdle

@BobMcArdle

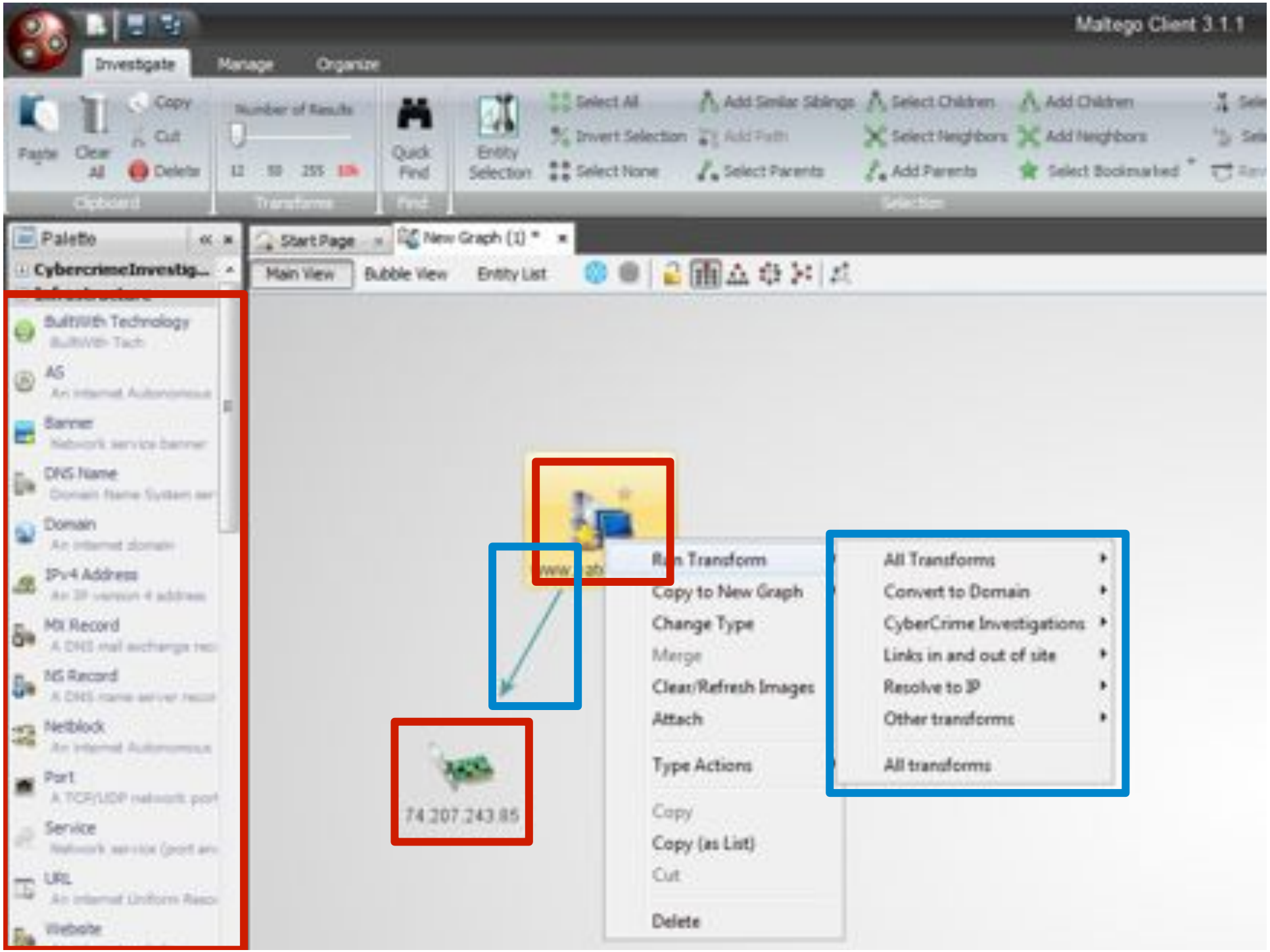
Cork | Sec

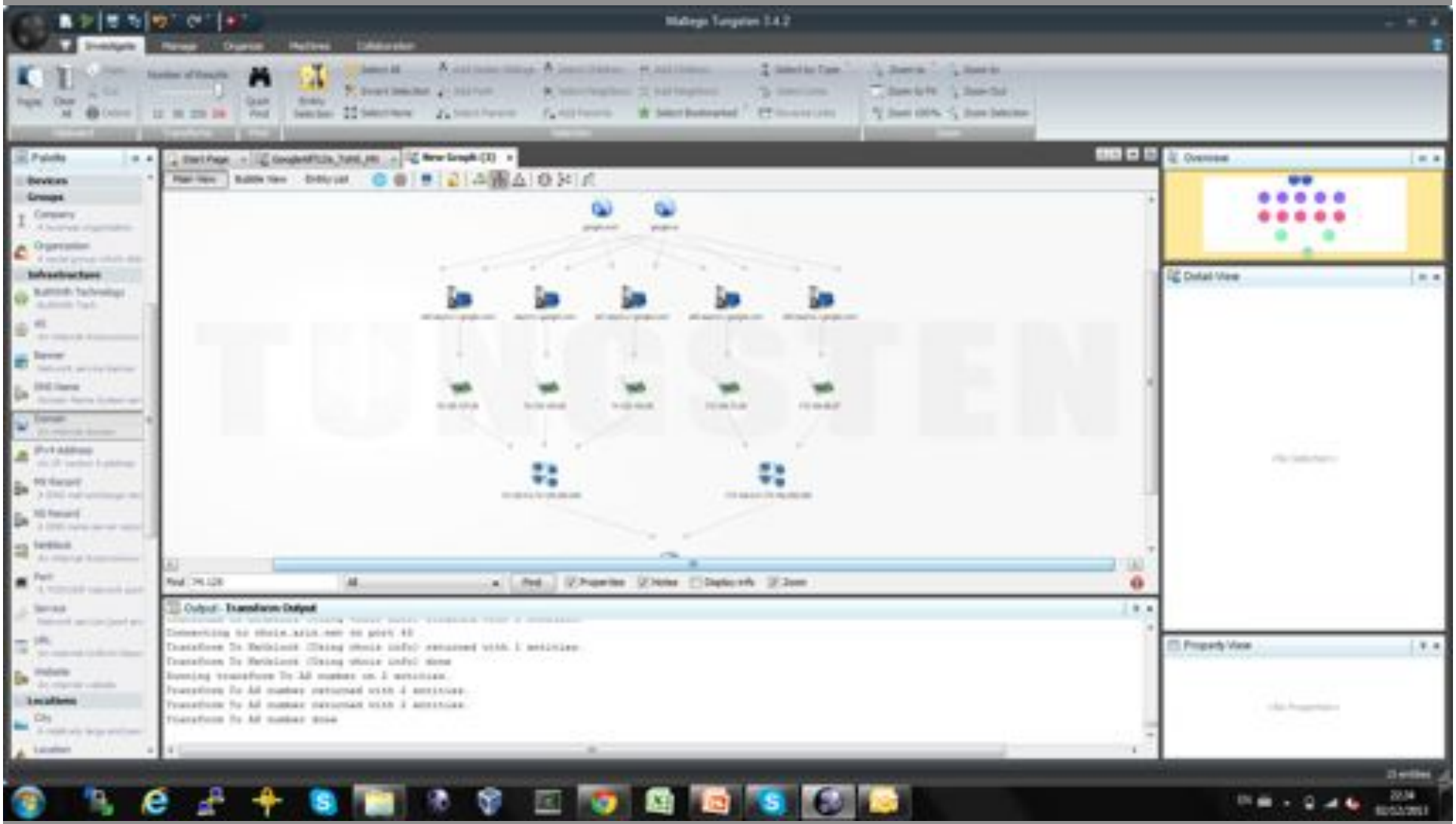

MALTEGO 3
OPENSOURCE INTELLIGENCE

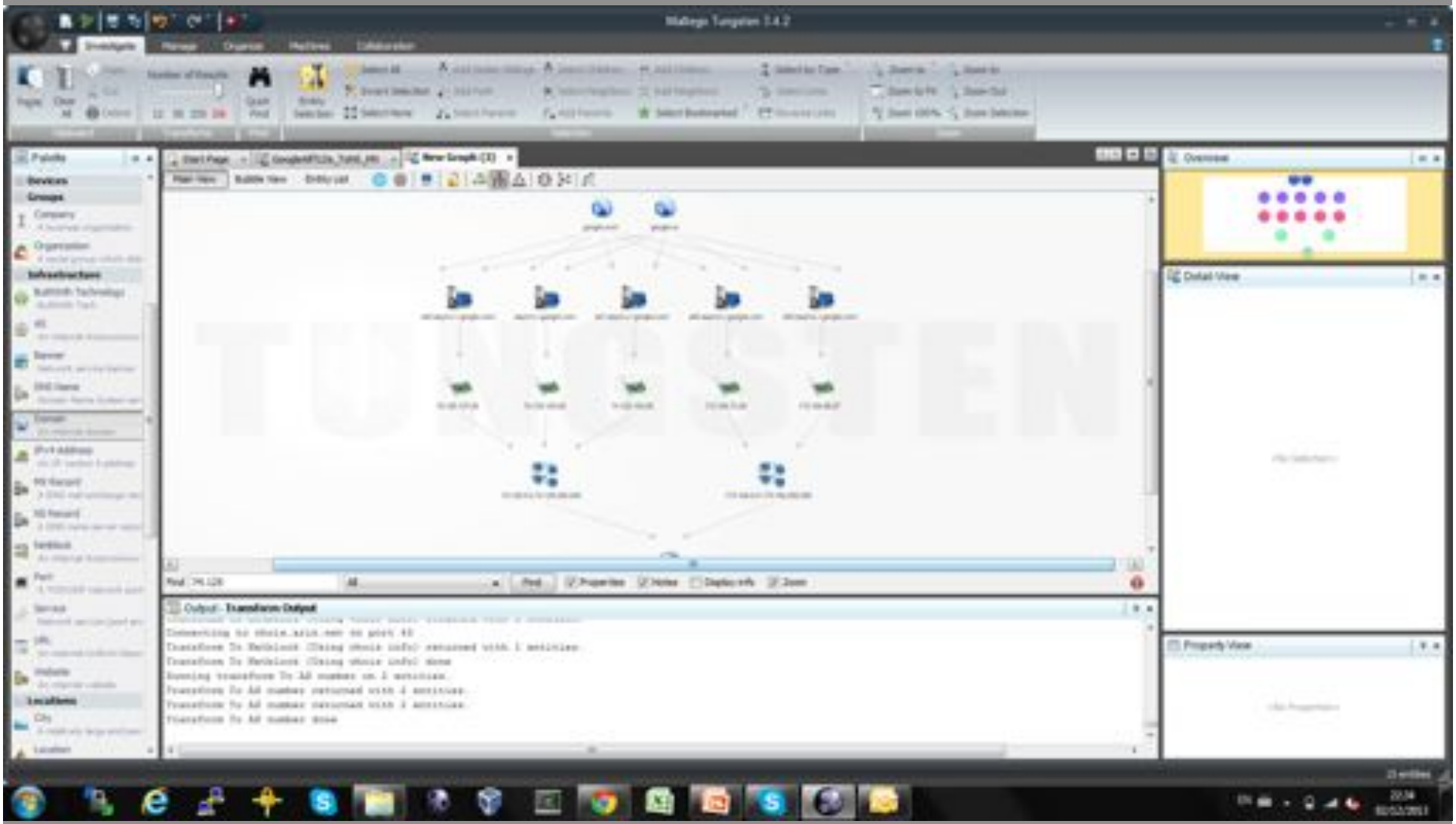

SEARCH
1,364 results for UCD
Advanced
Ireland
Current Company: University College Dublin
Reset
Premium Search
People
Relationship
Location
Ireland
Add
Industry
% Rights restricted by copyright; http: //iedr.ie/index.php/mnudomrega/mnudnssearch/96
% Do not remove this notice
domain: ucd.ie
descr: University College Dublin
descr: School/Educational Institution
descr: School/Educational Institution Name
admin-c: NOR3-IEDR
tech-c: NOR3-IEDR
registration: 04-April-1997
renewal: 04-April-2014
status: Active
nserver: auth-ns1.ucd.ie 137.43.132.53 2001:770:98:200::35:1
nserver: auth-ns2.ucd.ie 137.43.132.54 2001:770:98:200::35:2
nserver: sec-ns.tcd.ie
nserver: scrams.switch.ch
nserver: ucdp-gw-1.pa.dec.com
nserver: ucdp-gw-2.pa.dec.com
source: IEDR
person: Niall O'Reilly
nic-hdl: NOR3-IEDR
source: IEDR
person: Niall O'Reilly
nic-hdl: NOR3-IEDR
source: IEDR

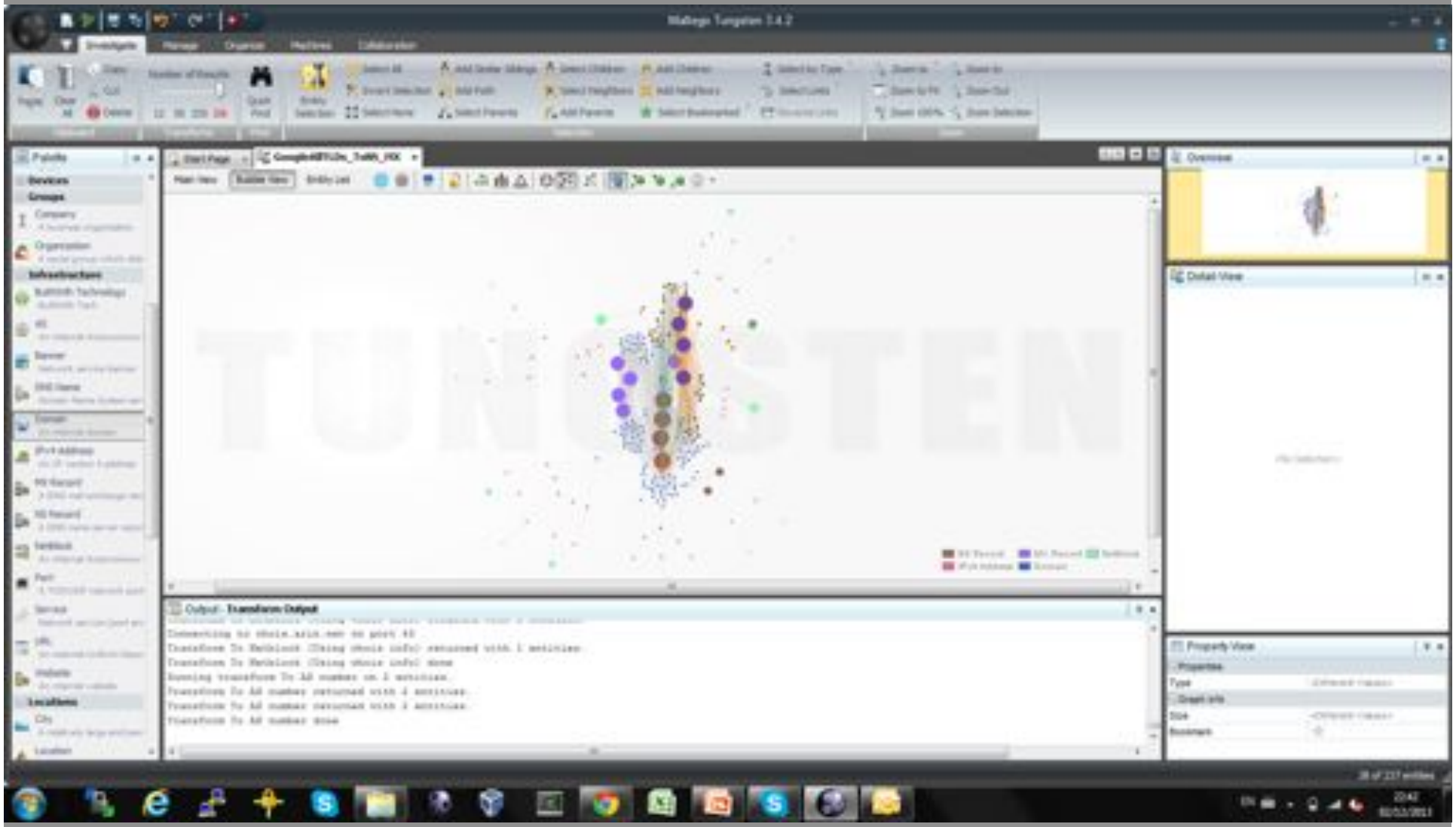
www.paterva.com

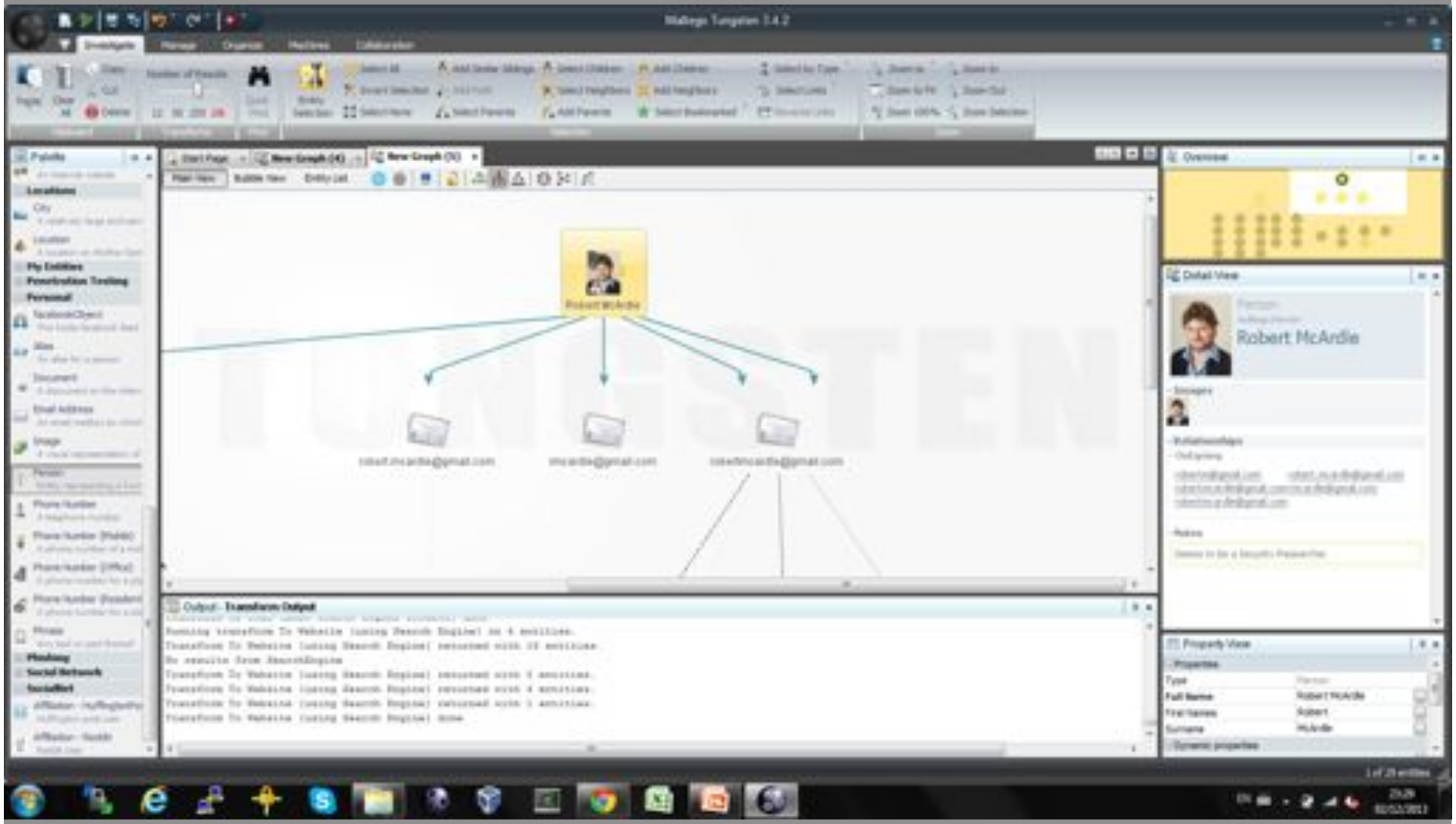
Maltego Basics


Maltego Client 3.1.1
Investigate
Manage
Organize
Palette
CybercrimeInvestig...
Start Page
New Graph (1) *
Main View
Bubble View
Entity List
BuiltWith Technology
AS
Banner
DNS Name
Domain
IPv4 Address
MX Record
NS Record
Netblock
Port
Service
URL
Website
Run Transform
Copy to New Graph
Change Type
Merge
Clear/Refresh Images
Attach
Type Actions
Copy
Copy (as List)
Cut
Delete
All Transforms
Convert to Domain
CyberCrime Investigations
Links in and out of site
Resolve to IP
Other transforms
All transforms
74.207.243.85

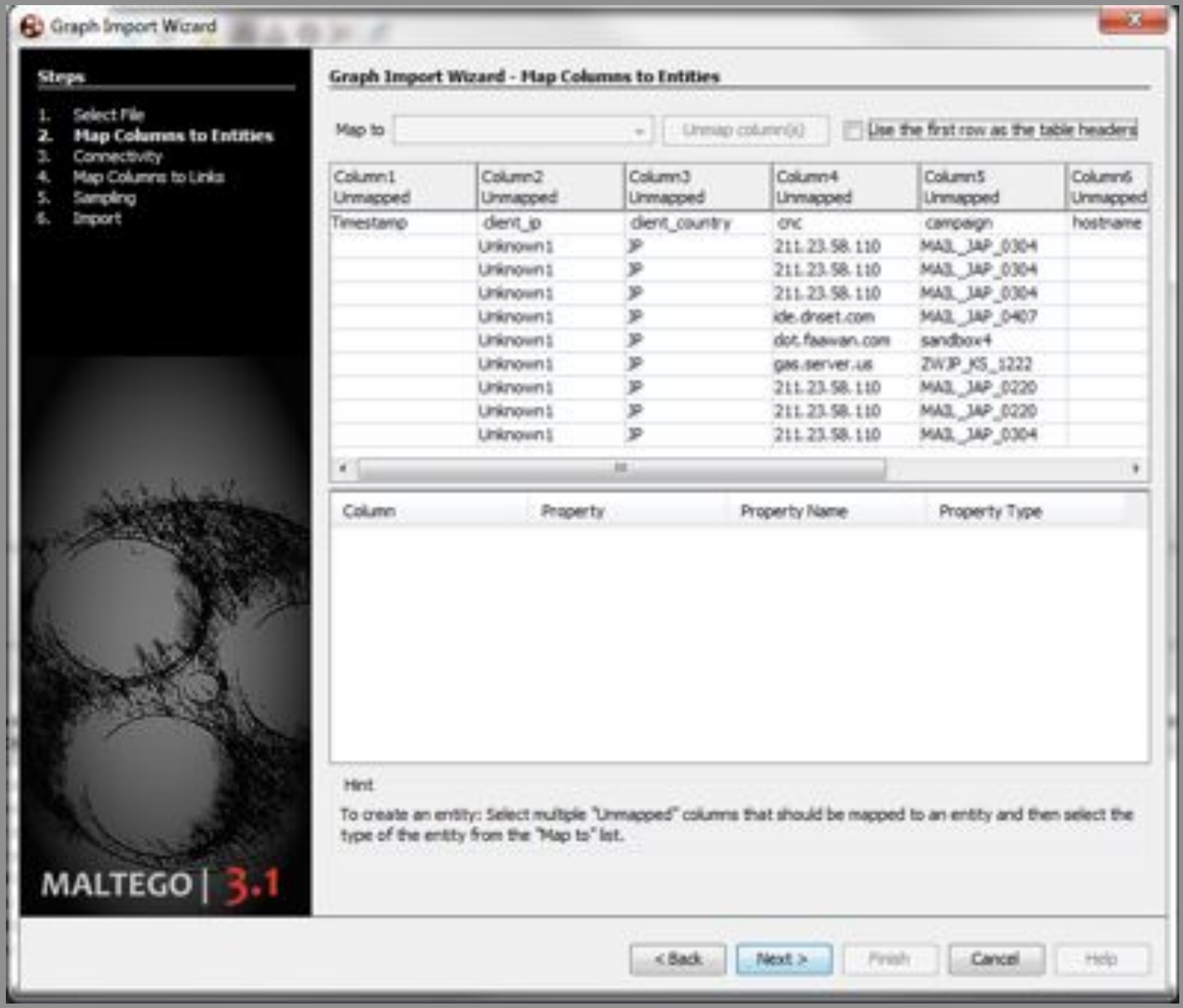


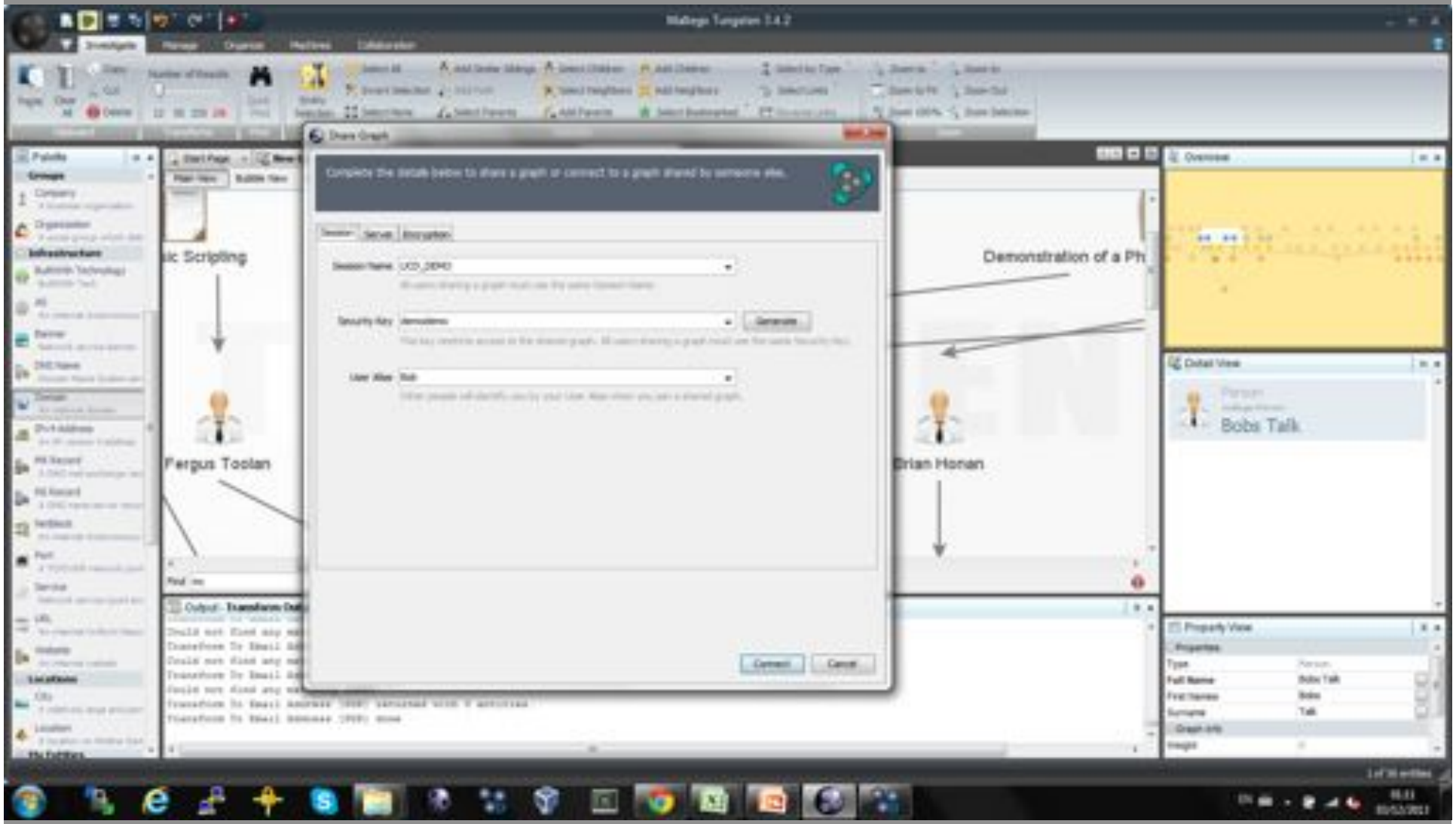



Maltego Tungsten 3.4.2
Investigate
Manage
Organize
Machines
Collaboration
Palette
Devices
Groups
Company
Organization
Infrastructure
Server
DNS Name
Domain
IPv4 Address
MX Record
NS Record
Netblock
Port
Service
URL
Website
Locations
City
Location
Start Page
Main View
Bubble View
Entity List
Overview
Detail View
Property View
Properties
Type
Graph Info
Size
Bookmark
Output - Transform Output
Connecting to whois.arin.net on port 43
Transform To Netblock [Using whois info] returned with 1 entities
Transform To Netblock [Using whois info] done
Running transform To AS number on 1 entities.
Transform To AS number returned with 1 entities.
Transform To AS number returned with 1 entities.
Transform To AS number done

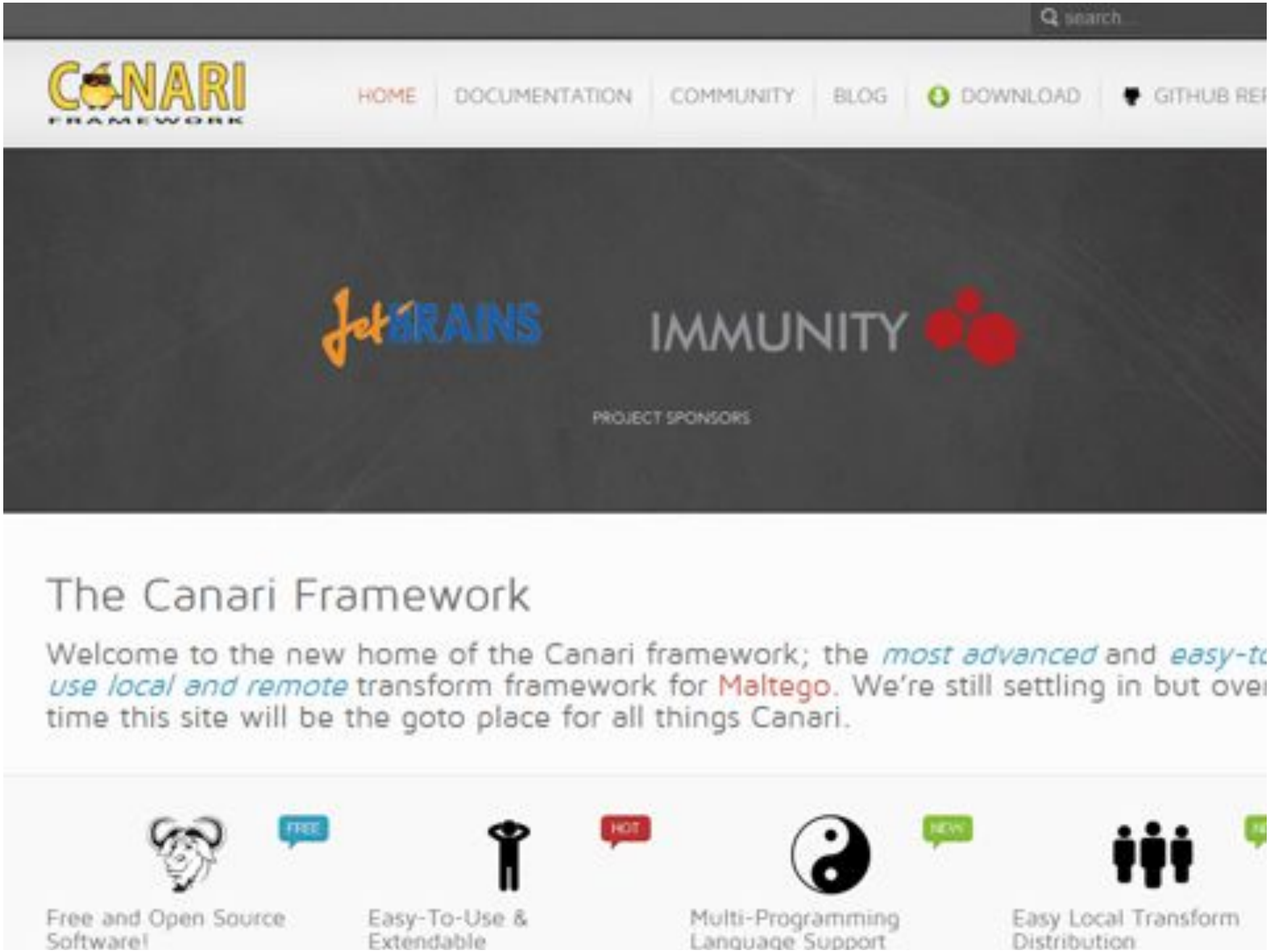

Maltego Tungsten 3.4.2
Robert McArdle
robert.mcardle@gmail.com
mcardle@gmail.com
roadmcardle@gmail.com
Overview
Detail View
Robert McArdle
Property View

Maltego Manual Mode / Collaboration


Graph Import Wizard
Steps
1. Select File
2. Map Columns to Entities
3. Connectivity
4. Map Columns to Links
5. Sampling
6. Import
MALTEGO | 3.1
Graph Import Wizard - Map Columns to Entities
Map to
Unmap column(s)
Use the first row as the table headers
Column1 Unmapped
Column2 Unmapped
Column3 Unmapped
Column4 Unmapped
Column5 Unmapped
Column6 Unmapped
Timestamp
client_ip
client_country
cnc
campaign
hostname
Unknown1
JP
211.23.58.110
MAL_JAP_0304
Unknown1
JP
211.23.58.110
MAL_JAP_0304
Unknown1
JP
211.23.58.110
MAL_JAP_0304
Unknown1
JP
ide.dnset.com
MAL_JAP_0407
Unknown1
JP
dot.faavan.com
sandbox4
Unknown1
JP
gas.server.us
ZWJP_KS_1222
Unknown1
JP
211.23.58.110
MAL_JAP_0220
Unknown1
JP
211.23.58.110
MAL_JAP_0220
Unknown1
JP
211.23.58.110
MAL_JAP_0304
Column
Property
Property Name
Property Type
Hint
To create an entity: Select multiple "Unmapped" columns that should be mapped to an entity and then select the type of the entity from the "Map to" list.
< Back
Next >
Finish
Cancel
Help


Share Graph
Complete the details below to share a graph or connect to a graph shared by someone else.
Session
Server
Encryption
Session Name
Security Key
Generate
User Alias
Connect
Cancel
Fergus Toolan
Brian Honan
Demonstration of a Ph
Bobs Talk

Extending Maltego - Seeds


search
CANARI
FRAMEWORK
HOME
DOCUMENTATION
COMMUNITY
BLOG
DOWNLOAD
GITHUB RE
JetBRAINS
IMMUNITY
PROJECT SPONSORS
The Canari Framework
Welcome to the new home of the Canari framework; the most advanced and easy-to
use local and remote transform framework for Maltego. We're still settling in but over
time this site will be the goto place for all things Canari.
FREE
HOT
NEW
Free and Open Source
Software!
Easy-To-Use &
Extendable
Multi-Programming
Language Support
Easy Local Transform
Distribution

PACKETNINJAS LLC

OFFENSIVE & DEFENSIVE SECURITY DISCIPLINES

HOME COMPANY SERVICES SOFTWARE RESOURCES

SocialNet

Packetninjas **SocialNet** searches common online social media outlets to provide automated searching for specific actors tied to online identities.

Pricing

- Local Law Enforcement - **$**1,000/year
- Federal Law Enforcement - **$**1,000/year* (federal will be changed to 2000/license in 2012)
- Trusted Investigators/Professionals - **$**4,000/year*

* Pricing can be billed on a per quarter basis if needed *

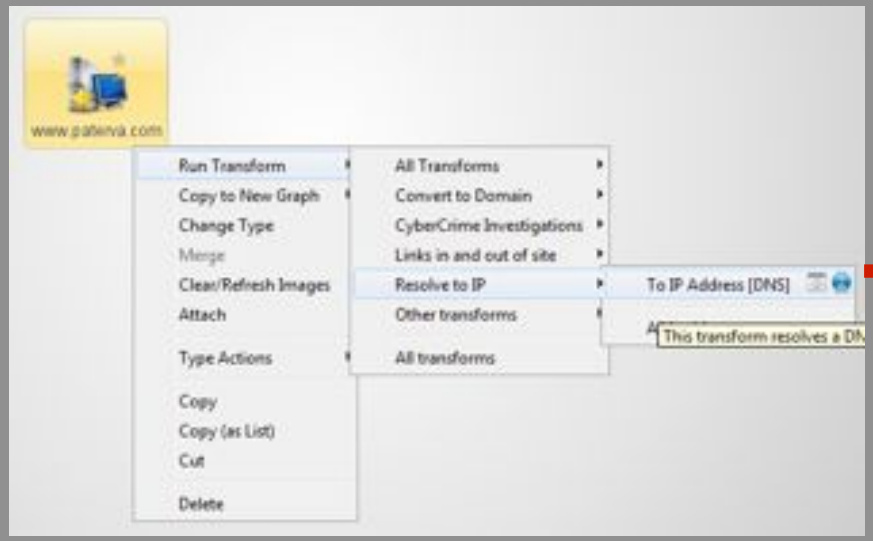
Please contact socialnet@packetninjas.net

DESCRIPTION

SocialNet is a SaaS based framework which currently integrates with Maltego to provide a robust set of commercially supported transforms for your investigators.

Extending Maltego – Do it Yourself


Local
VS.
TDS



https://cetas.paterva.com

www.yourServer.com

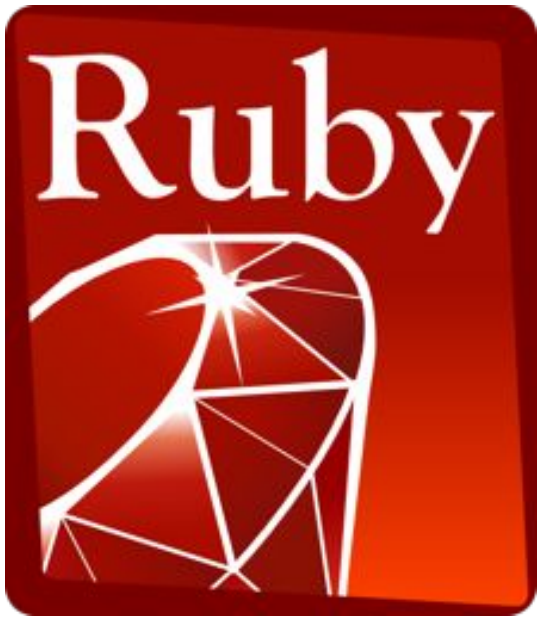
```
<MaltegoMessage>
  <MaltegoTransformRequestMessage>
    <Entities>
      <Entity Type="Maltego.Person">
        <Value>Robert McArdle</Value>
        <Weight>100</Weight>

        <AdditionalFields>
          <Field Name="person.fullname">Robert McArdle</Field>
          <Field Name="person.firstnames">Robert</Field>
          <Field Name="person.lastname">McArdle</Field>
        </AdditionalFields>

        <TransformFields>
          <Field Name="PGP Server URL">http://pgp.mit.edu:11371</Field>
        </TransformFields>
      </Entity>
    </Entities>

    <Limits HardLimit="50"></Limits>

  </MaltegoTransformRequestMessage>
</MaltegoMessage>
```

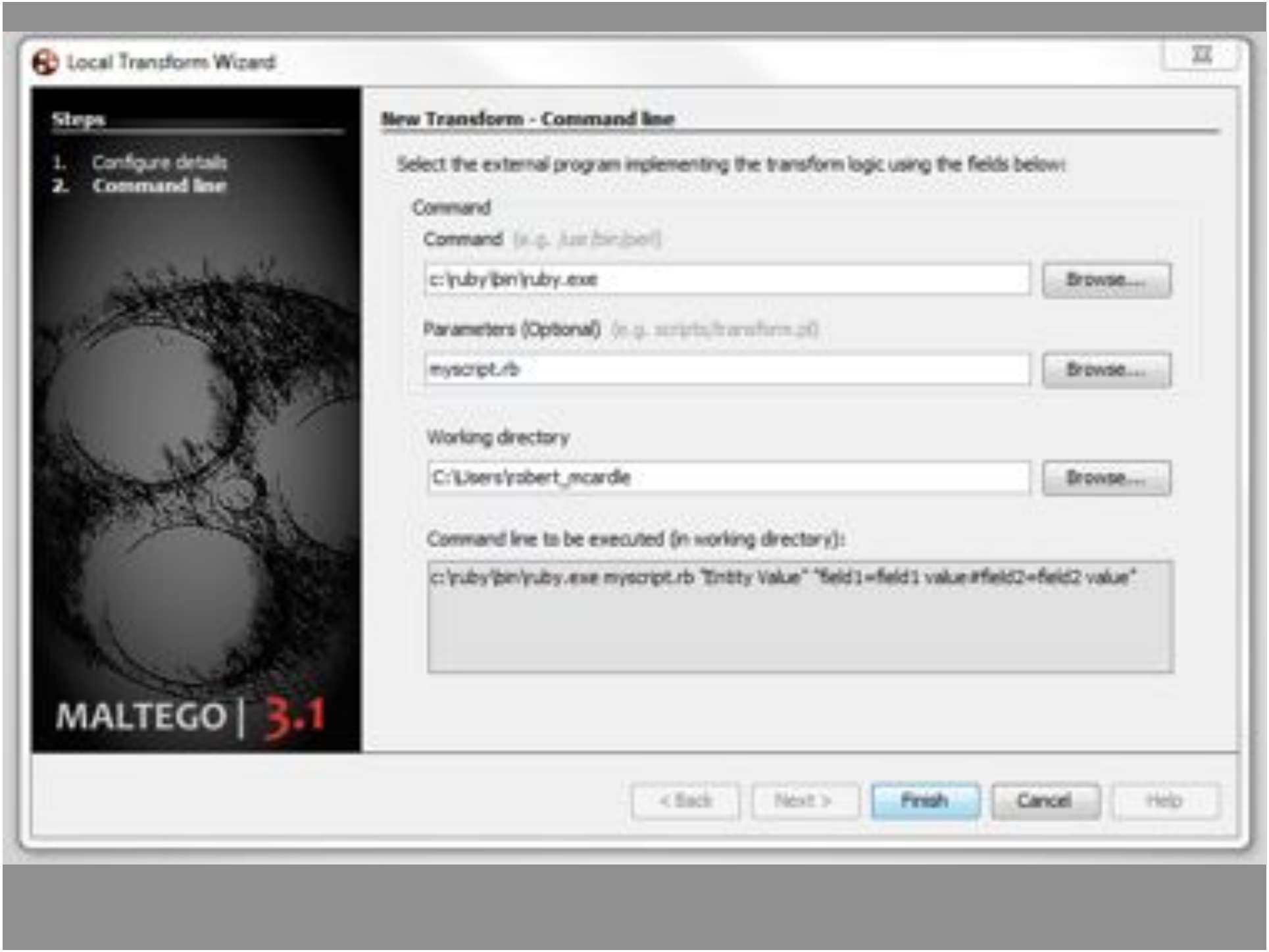
```
<MaltegoMessage>
  <MaltegoTransformResponseMessage>
    <Entities>
      <Entity Type="AffiliationBebo">
        <Value>Bennie van der Broekwurm</Value>
        <Weight>100</Weight>
        <DisplayInformation>
          <Label Name="Details" Type="text/html">
            <![CDATA[<html>MYHTML HERE</html>]]>
          </Label>
        </DisplayInformation>

        <AdditionalFields>
          <Field Name="uid" DisplayName="Unique identifier" MatchingRule="strict">334234110</Field>
          <Field Name="network" DisplayName="Network">Schmoep</Field>
        </AdditionalFields>

        <IconURL> http://network.com/people/334234110.png</IconURL>
      </Entity>
      <Entity>
        another one..
      </Entity>
    </Entities>
    <UIMessages>
      <UIMessage MessageType="Inform">Could only enumerate 20 entries</UIMessage>
    </UIMessages>
  </MaltegoTransformResponseMessage>
</MaltegoMessage>
```

XML Contents Output

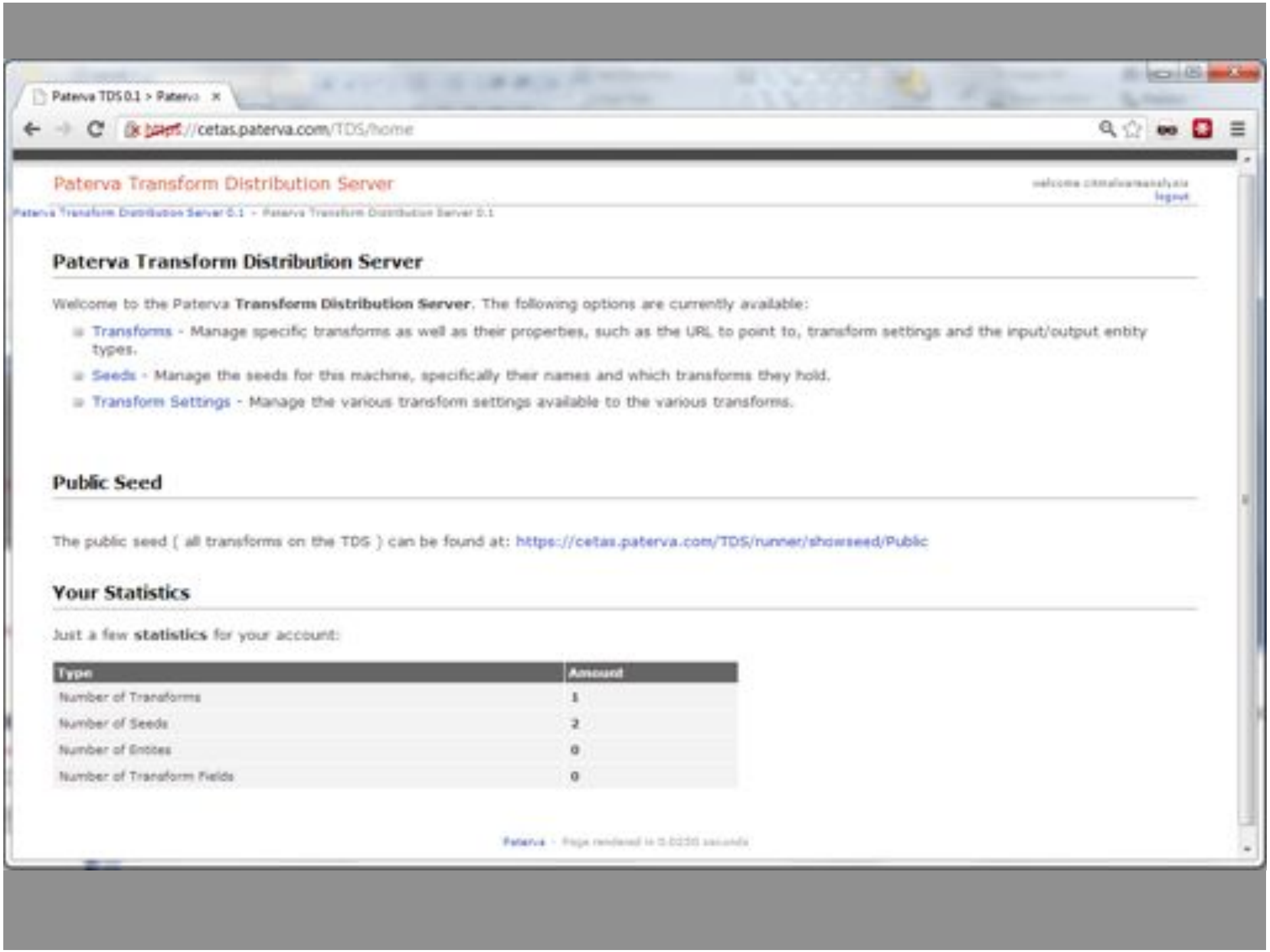

php

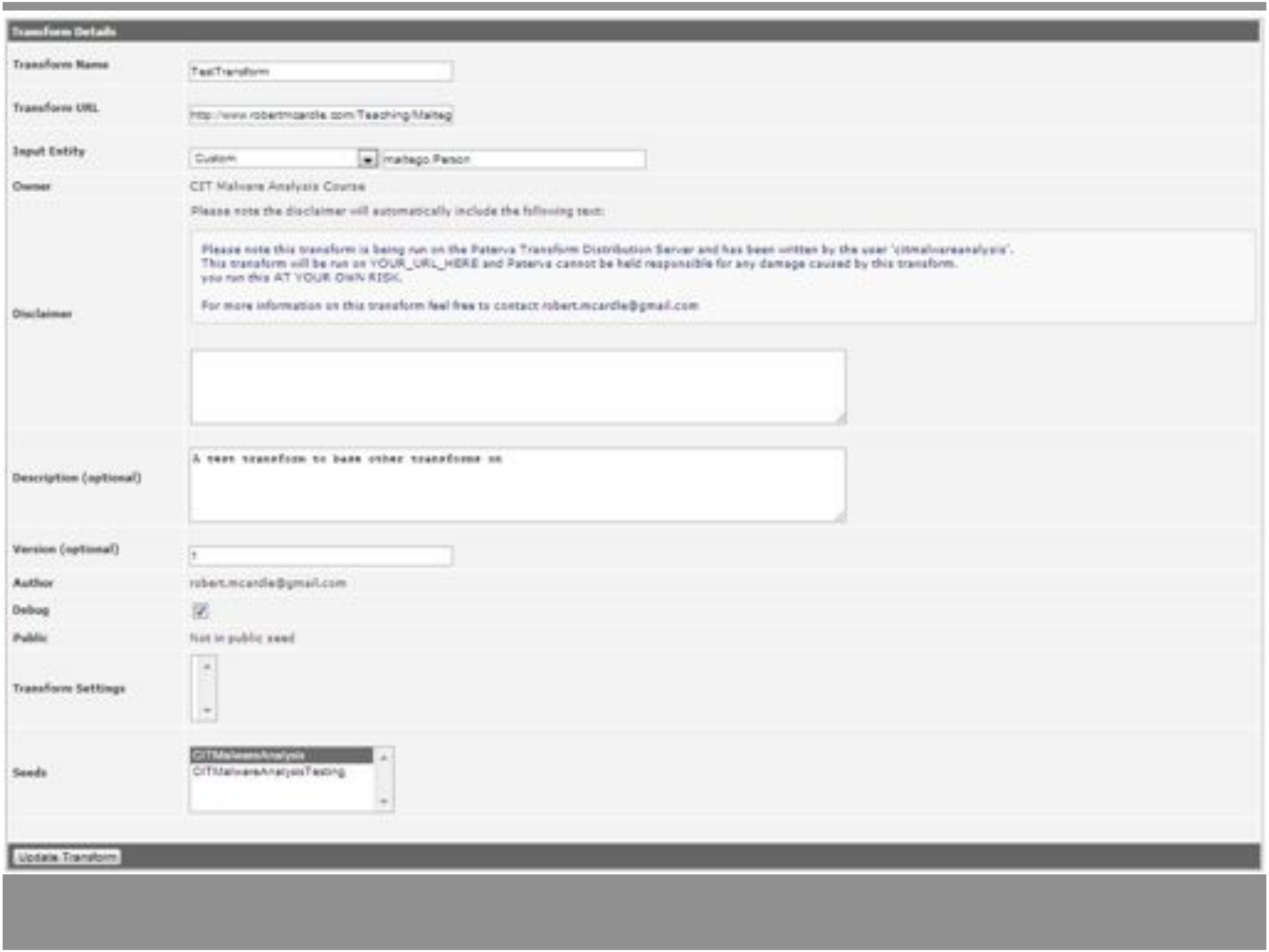

python


Ruby


Local Transform Wizard
Steps
1. Configure details
2. Command line
MALTEGO | 3.1
New Transform - Command line
Select the external program implementing the transform logic using the fields below:
Command
Command (e.g. /usr/bin/perl)
c:\ruby\bin\ruby.exe
Browse...
Parameters (Optional) (e.g. scripts/transform.pl)
myscript.rb
Browse...
Working directory
C:\Users\robert_mcardle
Browse...
Command line to be executed (in working directory):
c:\ruby\bin\ruby.exe myscript.rb "Entity Value" "field1=field1 value#field2=field2 value"
< Back
Next >
Finish
Cancel
Help

https://cetas.paterva.com/TDS/

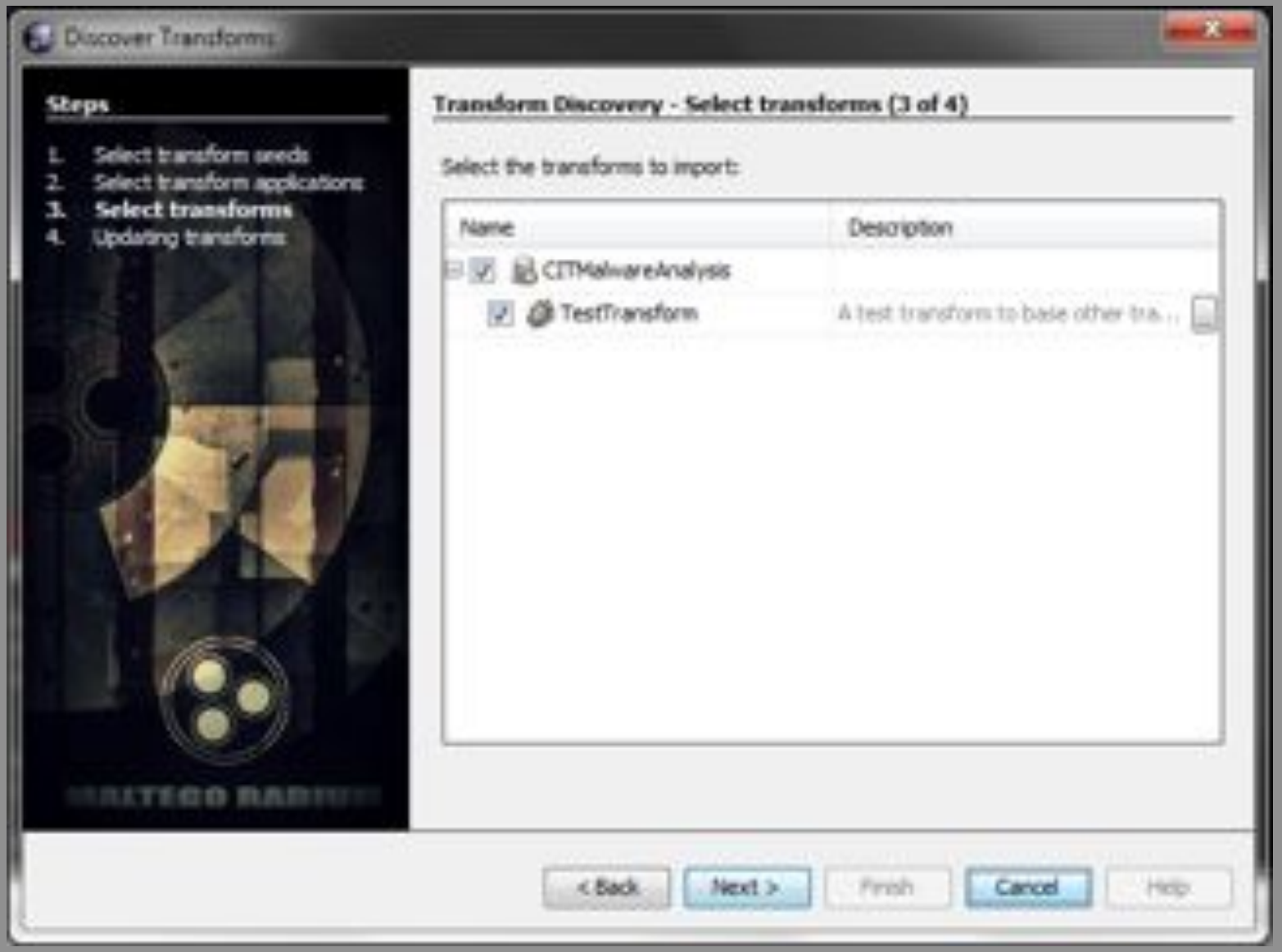

Paterva TDS 0.1 > Paterva
https://cetas.paterva.com/TDS/home
Paterva Transform Distribution Server
logout
Paterva Transform Distribution Server 0.1 - Paterva Transform Distribution Server 0.1
Paterva Transform Distribution Server
Welcome to the Paterva Transform Distribution Server. The following options are currently available:
Transforms - Manage specific transforms as well as their properties, such as the URL to point to, transform settings and the input/output entity types.
Seeds - Manage the seeds for this machine, specifically their names and which transforms they hold.
Transform Settings - Manage the various transform settings available to the various transforms.
Public Seed
The public seed (all transforms on the TDS) can be found at: https://cetas.paterva.com/TDS/runner/showseed/Public
Your Statistics
Just a few statistics for your account:
Type
Amount
Number of Transforms
1
Number of Seeds
2
Number of Entities
0
Number of Transform Fields
0
Paterva

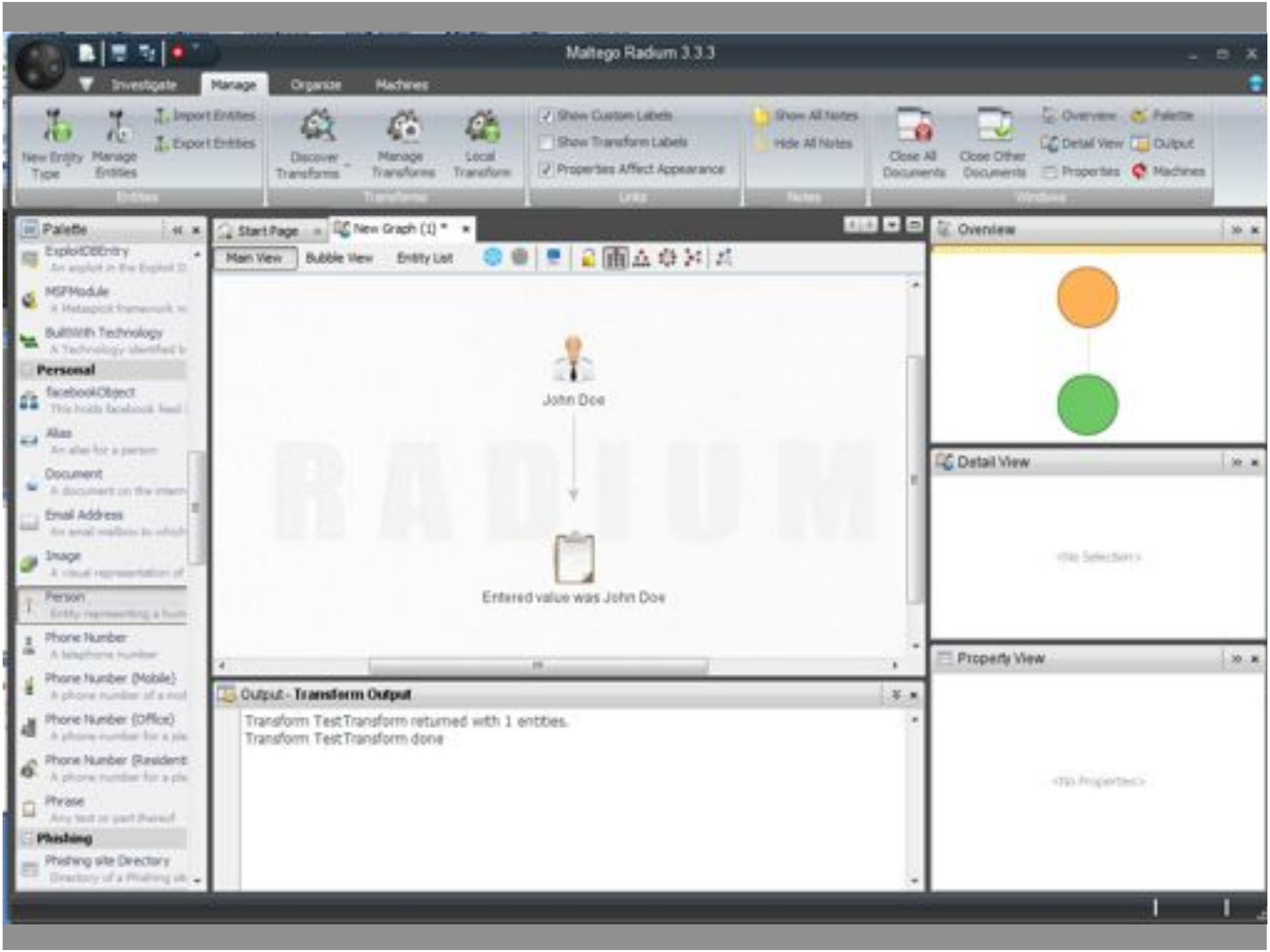

Transform Details
Transform Name
TestTransform
Transform URL
http://www.robertmcandle.com/Teaching/Maltego
Input Entity
Custom
maltego.Person
Owner
CIT Malware Analysis Course
Please note the disclaimer will automatically include the following text:
Disclaimer
Please note this transform is being run on the Paterva Transform Distribution Server and has been written by the user 'citmalwareanalysis'.
This transform will be run on YOUR_URL_HERE and Paterva cannot be held responsible for any damage caused by this transform.
you run this AT YOUR OWN RISK.
For more information on this transform feel free to contact robert.mcandle@gmail.com
Description (optional)
A test transform to base other transforms on
Version (optional)
1
Author
robert.mcandle@gmail.com
Debug
Public
Not in public seed
Transform Settings
Seeds
CITMalwareAnalysis
CITMalwareAnalysisTesting
Update Transform

XAMPP

linode.com

```php
<?php

//Include needed libraries
include_once("./Libraries/Maltego.php");        // Maltego Transforms

//set return content-type to be XML
header ("content-type: text/xml");

//*****************************************
//YOUR CODE GOES HERE
//*****************************************

//BASIC TRANSFORM
$maltegoTransformInput = new MaltegoTransformInput();
$maltegoTransformResponse = new MaltegoTransformResponse();
$maltegoTransformInput->getEntity();
$return_value = "Entered value was ".$maltegoTransformInput->value;
$ent = $maltegoTransformResponse->addEntity("maltego.Phrase",$return_value);
$maltegoTransformResponse->returnOutput();

?>
```

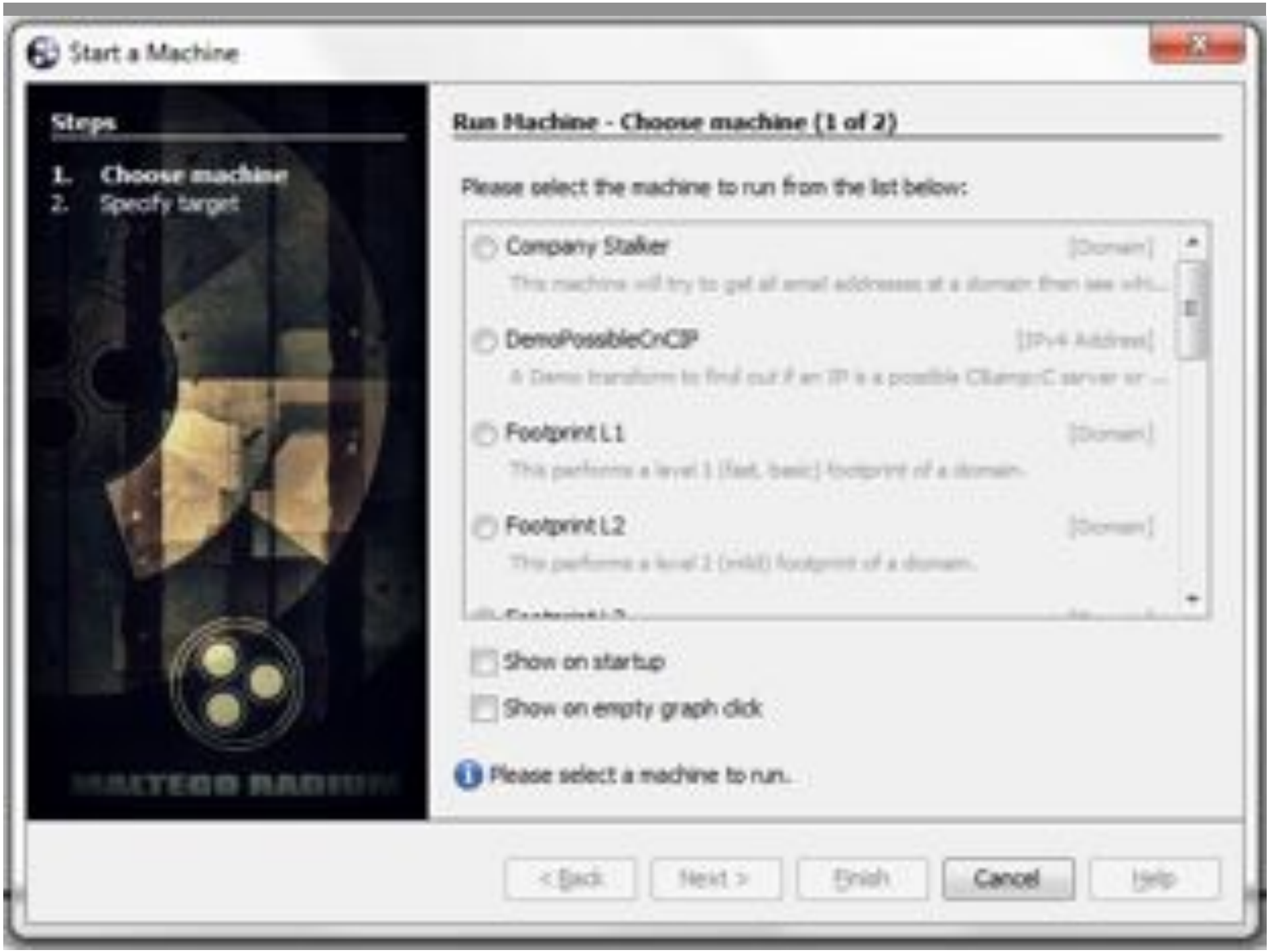

Discover Transforms
Steps
1. Select transform seeds
2. Select transform applications
3. Select transforms
4. Updating transforms
Transform Discovery - Select transforms (3 of 4)
Select the transforms to import:
Name
Description
CITMalwareAnalysis
TestTransform
A test transform to base other tra...
< Back
Next >
Finish
Cancel
Help


Maltego Radium 3.3.3
Investigate
Manage
Organize
Machines
New Entity Type
Manage Entities
Import Entities
Export Entities
Discover Transforms
Manage Transforms
Local Transform
Show Custom Labels
Show Transform Labels
Properties Affect Appearance
Show All Notes
Hide All Notes
Close All Documents
Close Other Documents
Overview
Detail View
Properties
Palette
Output
Machines
Palette
ExploitDBEntry
MSFModule
BuiltWith Technology
Personal
FacebookObject
Alias
Document
Email Address
Image
Person
Phone Number
Phone Number (Mobile)
Phone Number (Office)
Phone Number (Resident
Phrase
Phishing
Phishing site Directory
Start Page
New Graph (1) *
Main View
Bubble View
Entity List
John Doe
Entered value was John Doe
Output - Transform Output
Transform TestTransform returned with 1 entities.
Transform TestTransform done
Overview
Detail View
Property View

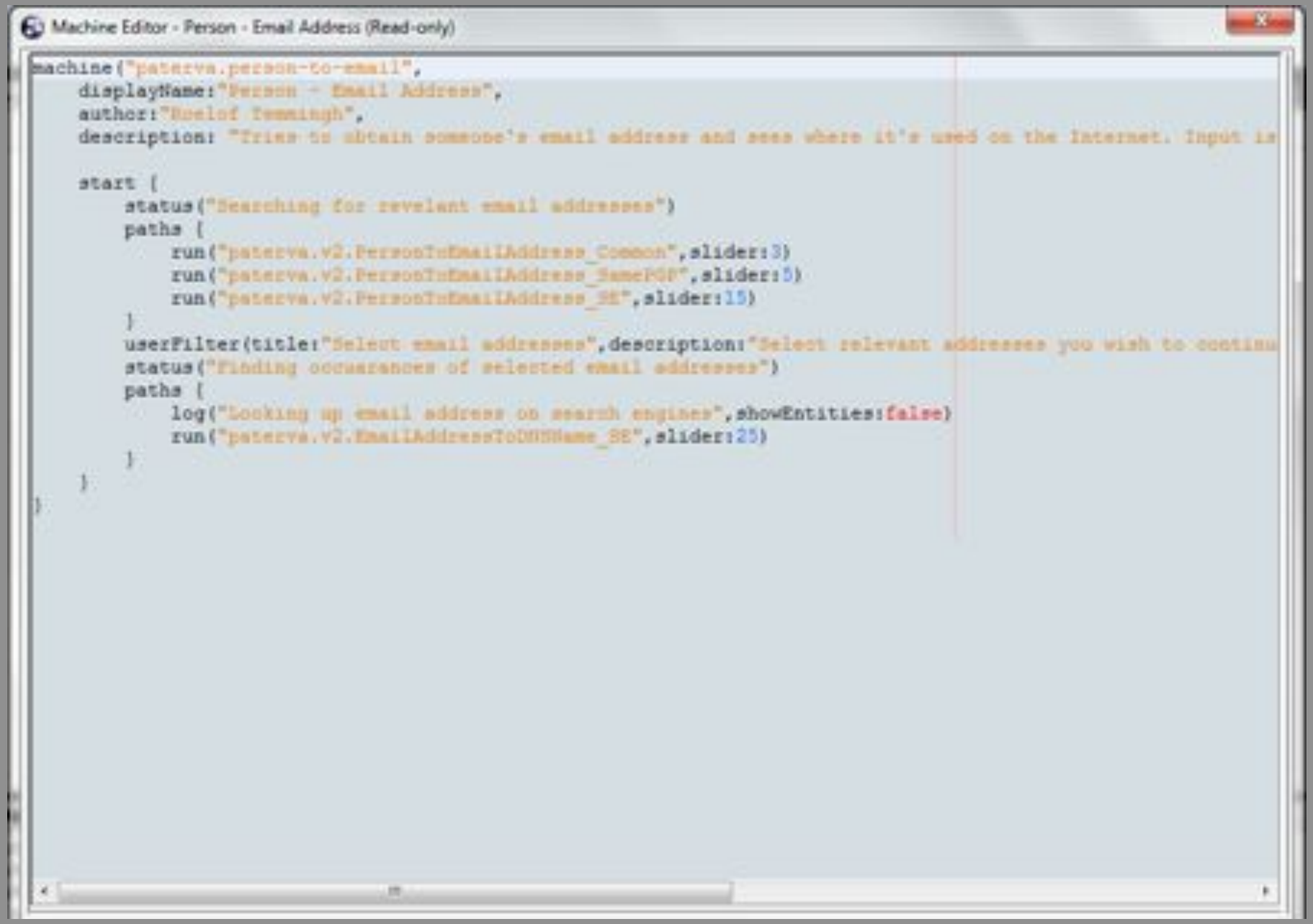
DEMO

DEMO

Automating Maltego - Machines

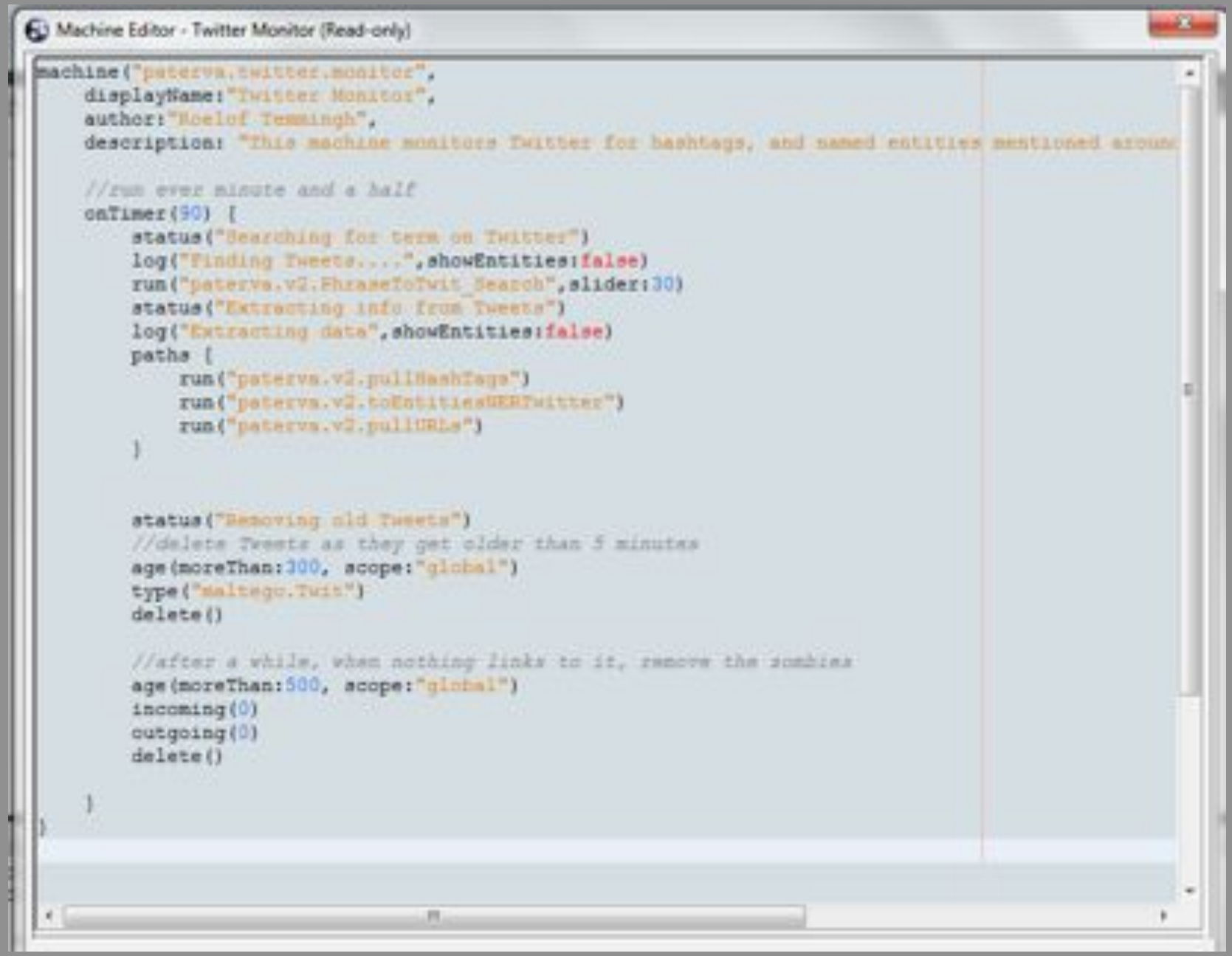

Start a Machine
Steps
1. Choose machine
2. Specify target
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Company Stalker
[Domain]
DemoPossibleCnC2P
[IPv4 Address]
Footprint L1
[Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2
[Domain]
Show on startup
Show on empty graph click
Please select a machine to run.
< Back
Next >
Finish
Cancel
Help

DEMO


Machine Editor - Person - Email Address (Read-only)
machine("paterva.person-to-email",
displayName:"Person - Email Address",
author:"Roelof Temmingh",
description: "Tries to obtain someone's email address and sees where it's used on the Internet. Input is
start {
status("Searching for revelant email addresses")
paths {
run("paterva.v2.PersonToEmailAddress_Common",slider:3)
run("paterva.v2.PersonToEmailAddress_SamePOP",slider:5)
run("paterva.v2.PersonToEmailAddress_SE",slider:15)
}
userFilter(title:"Select email addresses",description:"Select relevant addresses you wish to continu
status("Finding occuarances of selected email addresses")
paths {
log("Looking up email address on search engines",showEntities:false)
run("paterva.v2.EmailAddressToDNSName_SE",slider:25)
}
}
}

PATERVA

MALTEGO SCRIPTING LANGUAGE (1.1)


Machine Editor - Twitter Monitor (Read-only)
machine("paterva.twitter.monitor",
displayName:"Twitter Monitor",
author:"Roelof Temmingh",
description: "This machine monitors Twitter for hashtags, and named entities mentioned aroun
//run ever minute and a half
onTimer(90) {
status("Searching for term on Twitter")
log("Finding Tweets....",showEntities:false)
run("paterva.v2.PhraseToTwit_Search",slider:30)
status("Extracting info from Tweets")
log("Extracting data",showEntities:false)
paths {
run("paterva.v2.pullHashTags")
run("paterva.v2.toEntitiesNERTwitter")
run("paterva.v2.pullURLs")
}
status("Removing old Tweets")
//delete Tweets as they get older than 5 minutes
age(moreThan:300, scope:"global")
type("maltego.Twit")
delete()
//after a while, when nothing links to it, remove the zombies
age(moreThan:500, scope:"global")
incoming(0)
outgoing(0)
delete()
}
}

5 Golden Rules

- The real power is in the visualisation, not the OSINT transforms
- Don't be afraid to add manual information
- Delete entities you do not need – be ruthless.
- Embrace creating your own transforms
- Plan your approach before running a single transform.

Cork | Sec #7
(SNEAK PREVIEW!!!)
Jan 7th

Gerard Morris – "Anti-Piracy measures on Android"
Bob – "Augmented Reality"
Fabien Rabusseau – "VR Gaming" / Oculus Rift ☺

corksec.robertmcardle.com
Meetup.com/CorkSec