



In this 2 hour workshop we will take a look at the Maltego tool from Paterva.

Maltego is an open source intelligence and forensics application. It is an excellent tool for the mining and gathering of information and representing it in a easy to understand format.

Like most tools – the best way to get an idea what it can do is with plenty of examples, which is what we will be doing today

But first...two quick disclaimer. Firstly, I have **NOTHING** to do with the company that make Maltego. In fact I work for Trend Micro down in Cork. I have met the guys behind the tool in the past, and use it extensively as part of my work. But apart from simply thinking that the tool is awesome and more people should know about it, that's where my connection to Maltego ends.

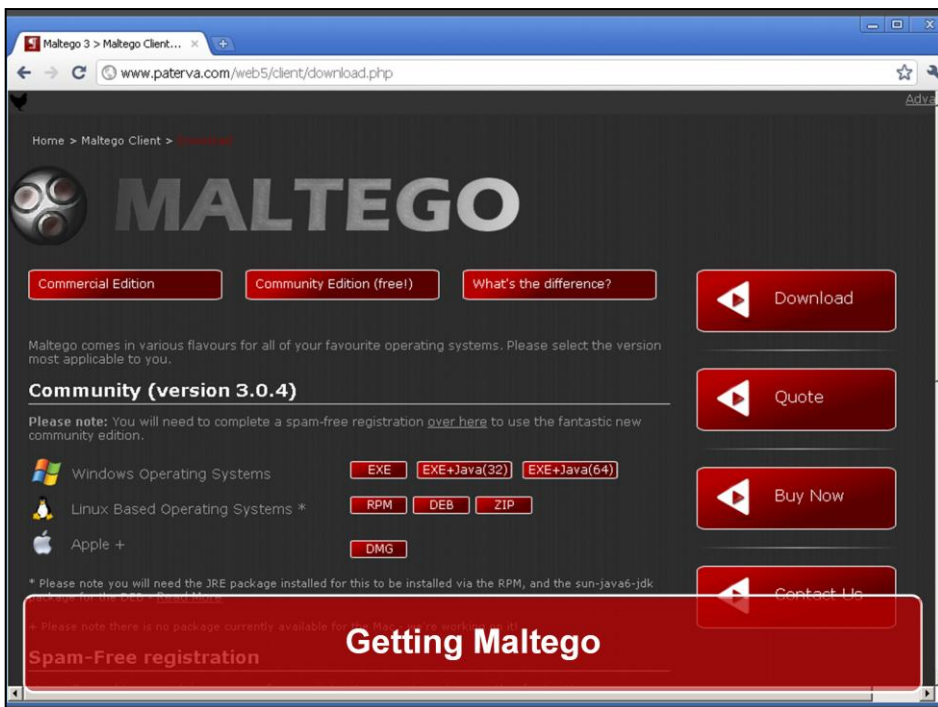
DISCLAIMER NOTICE

**Presentation contains
live demos which are
prone to embarrassing
failures.**



Secondly this presentation use lots of live demo, and very little powerpoint. These live demos are also heavily reliant on the venues stellar Wifi network, and on servers on the internet that are completely beyond my control.

You have been warned 😊



First up – how to get the tool. I'll be showing lots of examples during this session – so its worth getting a copy of Maltego so that you can follow along with me. Alternatively I'll make the slides available after the session, so that you can try things out in your own time.

You can download Maltego from **www.paterva.com** . In addition to the Maltego software you will also need to install Java, and have an internet connection. Luckily the tool is available for Windows, Linux and Mac.

Maltego also comes in two flavours – the Commercial version and the Community version. There are a couple of differences between the two (which you can see on the Maltego site) e.g. the commercial version is faster, will return more results, and the community version is not constantly updated. You also need to register the community version to use it.

For now I recommend that if you want to follow along – download the community version, and install it and register it.



Open Source Intelligence (OSINT)

So I mentioned that Maltego is an open source intelligence tool – but what is that, and why should you care? Some people get mixed up here and think this means the tool is Open Source – its not. Open Source Intelligence is all about intelligence gathering from public or non covert channels.

The web is full of all sorts of incredibly useful information – just waiting to be queried, and all publically available.

Think of public information on people online – twitter accounts, facebook account, linkedin and any number of other pages – all with a wealth of freely available information. Obviously this will work better against people of a certain age group – the so called Generation X and Generation Y of this world are much more likely to have left traces online. It also does not work as well against members of the security community – or at least I hope it doesn't ☺

With tools like Google Maps and Earth we can visit anywhere in the world, without leaving the browser. You can view someones office, and all of the surrounding buildings – very useful for social engineers.

And what about websites – with a few simple searches in right locations you can find out contact details, IP ranges, physical locations and lots more

The fact is that the web has an awful amount of useful information. 1.7 Million Terrabytes of information is uploaded every year. Burn all of that onto DVDs and they would stretch into space. We want to use Maltego to map the relationships between this information



As we all know Websites are made up of links. Each link joins one website page with another.

Each of these websites is essentially a chunk of information, which may or may not be useful to us. For a minute lets think of these chunks of information as “Entities”

But websites are not the only Entities linked together on the web – there are lot of other interesting things floating around out there

-Domains, DNS Names, IP Addresses, Emails, Tweets, People, Documents etc

And all of these pieces of information are linked together – either in a rigid man-made way, or sometimes using fuzzier approaches.

Example (Rigid / Man-Made link)

- DNS Name -> IP Address
 - www.issaireland.org -> 209.61.216.49
 - The "link" in this case is DNS

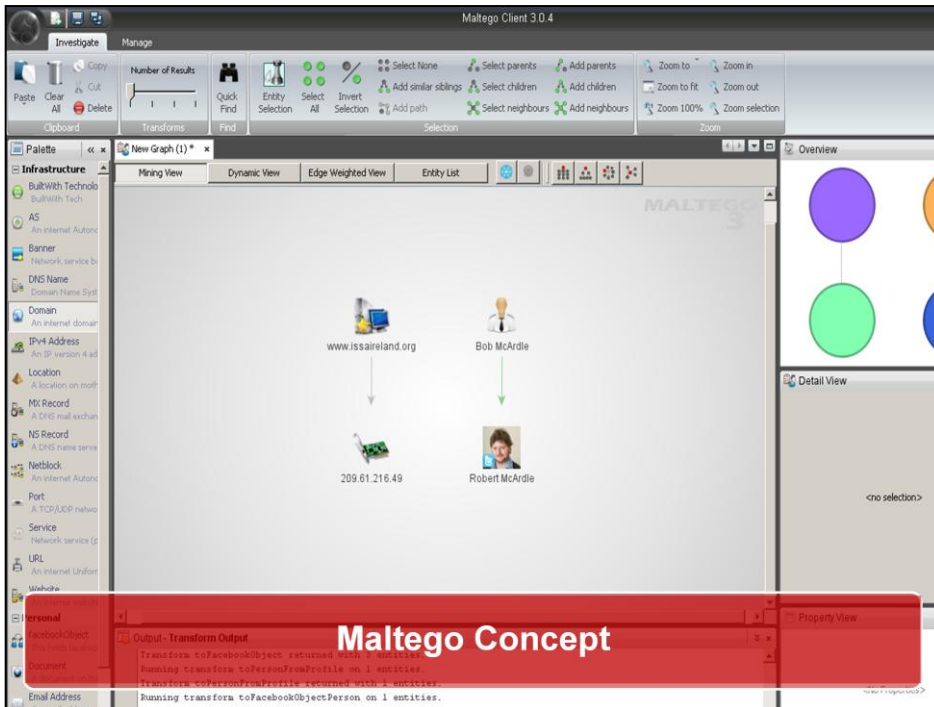
Example (flexible / fuzzy link)

- Persons Name -> Email Address
 - Robert McArdle -> RobertMcArdle@gmail.com
 - The "link" here is a website mentioning both close together
 - Not 100% certain / Fuzzy

What are you talking about?

That's sound fluffy – but what am I really talking about.

Lets take some examples



So what does that mean for Maltego

In Maltego there are two fundamental concepts

- We have **Entities** - Think of these as “things” or “pieces of information”. Examples would be People, Websites, IPs, Social Networking Accounts, Phone Numbers...

-And we have **Transforms** – Take an Entity and “transforms” it into other entities of some sort. Examples would be DNS Resolving (Website->IP), Searching for Social Network membership (Email->Myspace account) and so on.

How the Transforms are actually carried out can vary considerably – it might be a simple DNS lookup, a Google search, or a complex series of searches and queries across multiple sites.

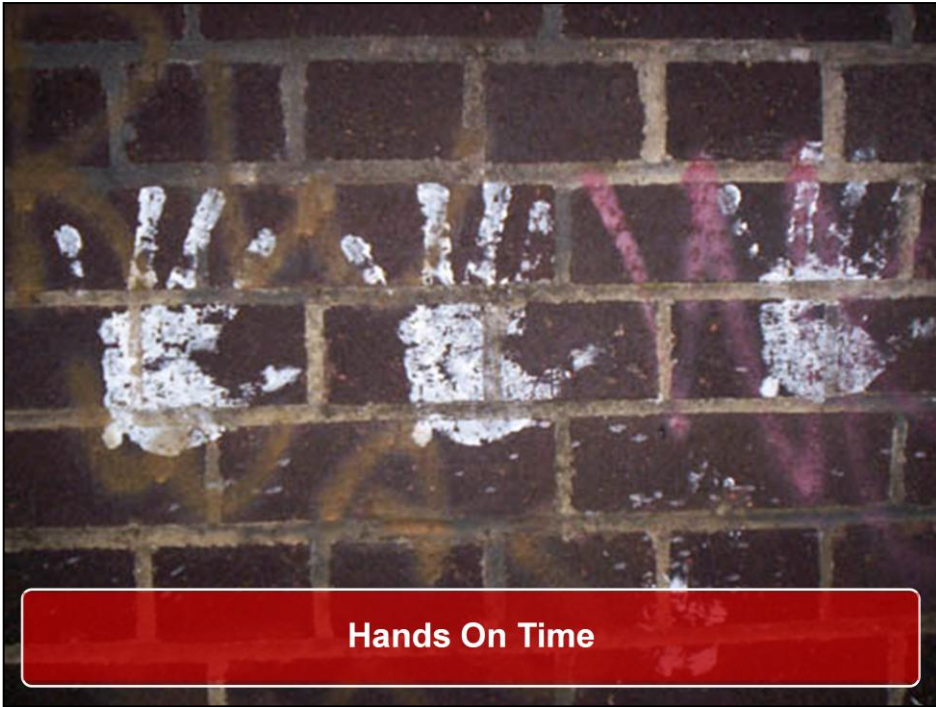
Maltego helps us to graph these relationships in a visible way we would never have been able to see with manual searching, in a search engine like Google. Look at the examples above – we have taken the Entity www.issaireland.org and transformed it into a IP address. That was a simple DNS Lookup. On the other hand we have the person entity Bob McArdle and we have transformed him to a Twitter entity. That involves using some of the Twitter query apis.

It is this combination of Man & Machine that makes Maltego so powerful

-Machines are great at running large automated tasks (i.e. Our transforms).

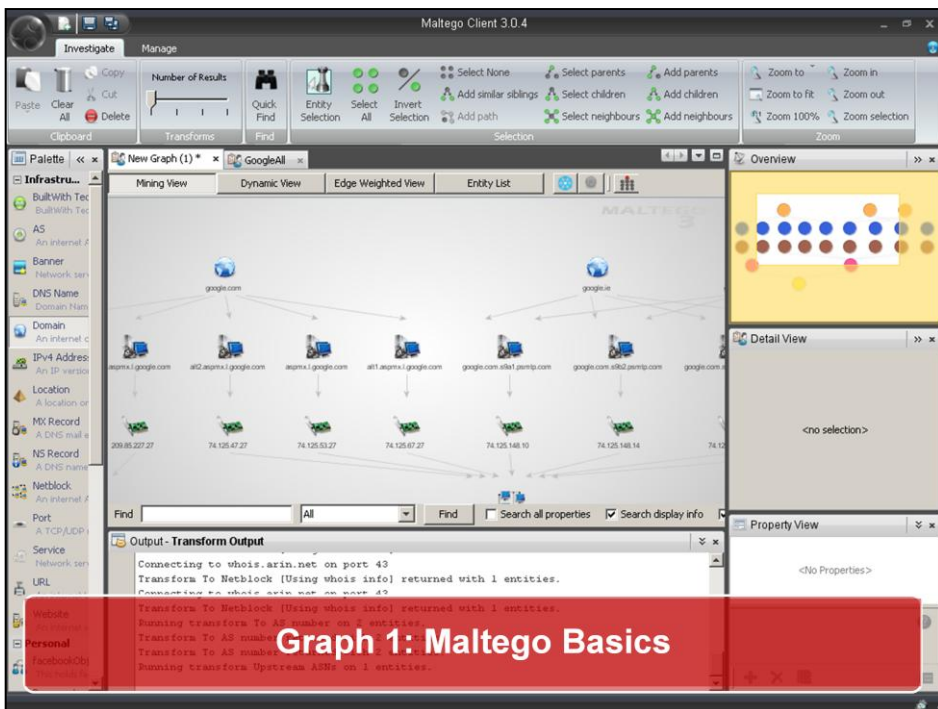
-Humans are excellent at Pattern Recognition

Now everything above is pretty simplistic – so lets do some hands-on demos to really put Maltego through its paces.



Ok so that's the concept – but there's no fun in me just standing here and showing slides, let take the Tool and show some cool examples – and you can follow along!

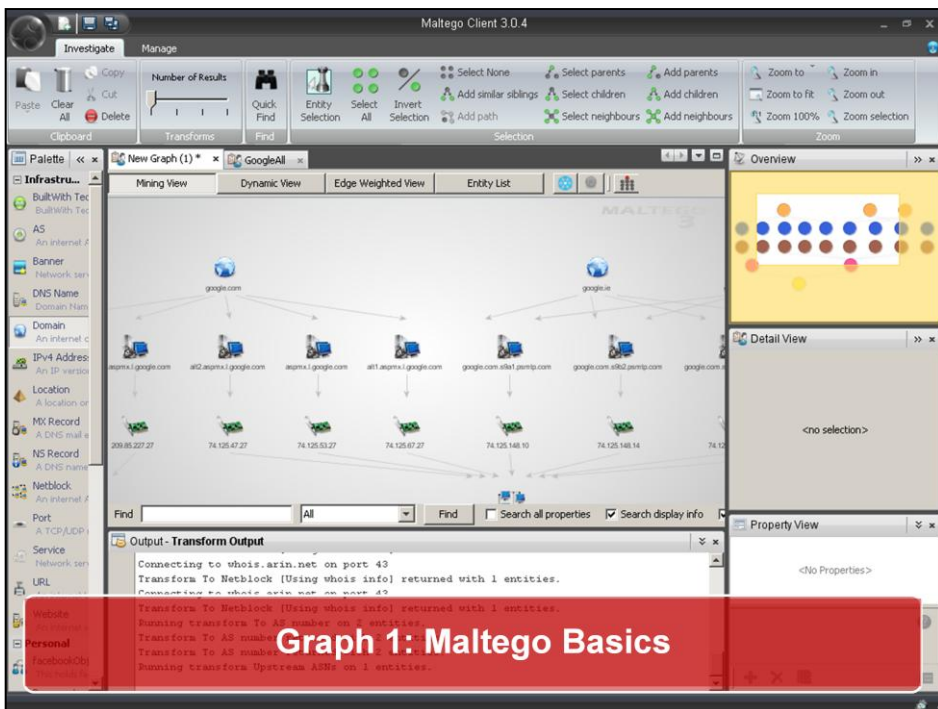
You may notice that my version of Maltego has some extra options compared to your versions – don't worry, all will be explained in time!



Hand-On 1 (Part 1)

For our first hands-on, let's try something really simple – just to get used to the Maltego GUI. When using Maltego I always find it useful to decide on what question I am trying to solve in advance. This time my question is simply going to be **“What Mail Servers does Google.com use, and what IP addresses are they on?”**

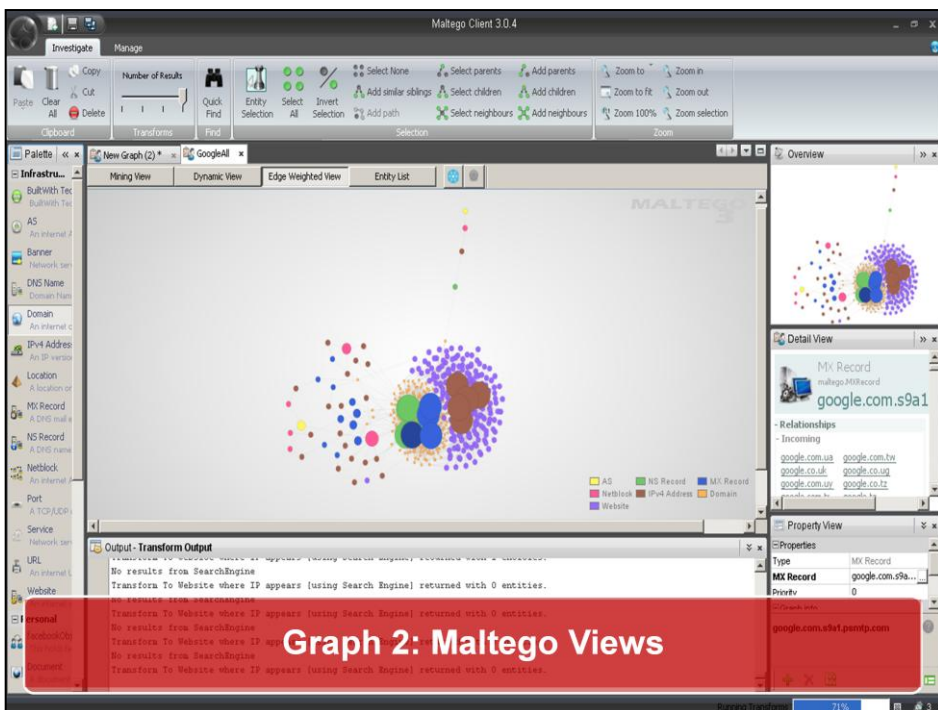
- First we create a new graph. There is a button in the top left corner (near the save icons), in the main menu, or just press Ctrl+T
- Next we will need a Domain entity. You will see a list of entities in the palette on the left of the screen. Let's drag a domain entry into the main screen area. Let's change the name to google.com – either by double clicking on the entity, or pressing F2
- To see what transforms are available for Domain entities, simply select the Entity, and right-click and select “Run Transform”. To make things easier to navigate Maltego places similar transforms into “Sets”. For our example we want to run the “To DNS Name – MX Server” transform, which is in the “DNS from Domain” set. Hovering over a set or transform will give you a little tooltip giving an overview of what the set or transform does. There are also two little buttons, the blue Information button (which brings you to a site explaining the transform), and settings button where you can configure transform settings (if any)
- Once the transform completes you should have a number of new MX Record Entities linked to the google.com domain. Now we want to find the IP addresses for these Records. You can select multiple entities by left clicking the mouse and dragging a box around them, or using Shift+Click to select each one. You'll notice that the MX Record entity has a different list of transforms to the Domain entity. The transform we want this time is the “Resolve to IP” transform. This is interesting – all the MX Records resolve to different IP addresses, in two main netblocks – but they all end in .27
- Let's make the graph more interesting – let's do the exact same transforms for google.ie to see if it shares the same IPs (drag another domain into the graph). Turns out google.ie uses different MX Records (on the psmtip.com domain – which comes from Google's acquisition of Postini), but the IPs are still on Google's netblocks
- Let's do the same for google.co.uk – turns out it uses the same MX Servers as google.ie



Hand-On 1 (Part 2)

- Lets do one last transform here – transform the Ips to Netblocks. There are a couple of transforms for this but for now lets use “To Netblock using WhoIS Info” (under Other Transforms). You will also notice the “All in this set” option which can be useful in some cases. Both of these Netblocks are on ASN 15169 – which belongs to Google
- Now we have covered a basic transform – lets look at some of the rest of the GUI
 - We’ve covered the Palette on the left, and the main graphing view in the middle
 - The bottom shows the output of your transforms
 - In the top right is the overview of the graph, which can also be used as a navigator
 - Below that is the very useful Detail view. Select an MX Record – you can see all incoming / outgoing links, the transforms that created them (and when). Depending on the transform – there might also be links to other sites. If you select multiple entites the detail view will show a list of them
 - Last for now is the property view – some entites will have additional properties – take a look at the Netblocks for example

- Before we move onto the next demo, let me show you a couple of ways to move around the graph. Select any entity – press Up to go to one of the entities parents, and down to go to one of its children. You can also press CTRL+UP to select ALL parents, or CTRL+SHIFT+UP to do the same but keep the current entity selected. All of this can also be done via the Selection Pane at the top – which also includes the very handy “Invert Selection”
- Lastly there is also a search option (CTRL+F or click “Quick Find”). For example search for all IP addresses beginning with 74.125.148 . This is very useful for larger graphs.
- Now lets save this graph and move on (My copy is available in **Demo1.mtgx**)



One of the most powerful components of Maltego are the different “views”. To show these off, lets take a bigger version of the graph we just created for Google. I took all 185 Google TLDs and for each of them found the corresponding mail server, name server and IP address. You can download the graph from <http://www.robertmccardle.com/maltegoworkshop/graphs/GoogleAll.mtgx>

So lets look at the views that are available in Maltego

- As you can see in this graph there are so many entities that Maltego no longer shows the individual values – instead colour coding them by entity type. You can zoom in and out of the graph using the scroll wheel on a mouse (or the buttons in the Zoom pane at the top), and move around the map by holding down Right click and dragging.

- The default view is called “**Mining View**”, which is perfectly fine for smaller graphs where the details really matter. For larger graphs like this one, we have other ways of viewing the data. Within Mining View there are 4 possible layouts (try these out)

- Block Layout:** Default layout for mining view. Entities are grouped together by Entity type

- Heirarchical Layout:** Think of it like a tree based layout, like a file manager – Each entity is grouped with respect to its parents and children

- Centrality Layout:** Entites that are most central to the graphs (most incoming links) appear in the middle, with others scattered around. This is a good layout for spotting anomalies. For this graph we can see one such anomaly – which will become more evident in further views – of all the Google TLDs, .dz is unique in that it uses a Name Server that no other domain does. .dz is the TLD for algeria

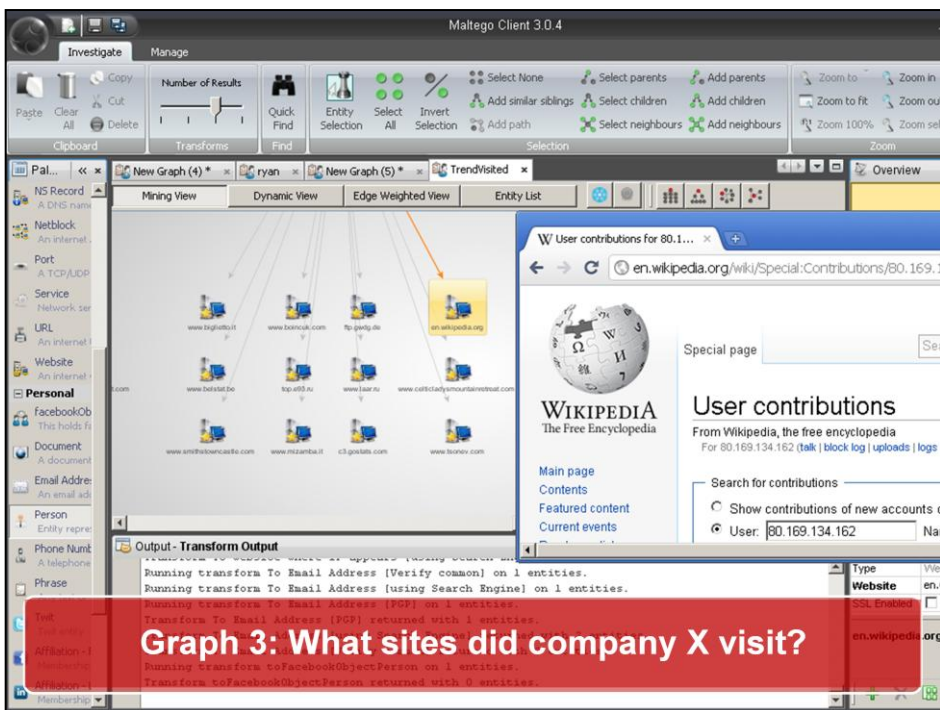
- Organic Layout:** Nodes are packed tightly together to minimize distance between them

- The second view is called “**Dynamic View**” - here entities that are calculated to be more central to the graph are given larger nodes. Here we can a large amount of Websites clustering around the same 4 IP addresses, and a lot of domains clustering around some MX and NS records. Its hard to make out what is going on in these clusters – but it is easier to look at the “anomaly” parts of the Google backend. Dynamic view is a great view for looking for the stranger parts of a graph. (Look at Google.cn sticking out from the crowd)

- The third view is called “**Edge Weighted View**” – Here node sizes are based on the number of incoming links – allowing you to figure out the most linked to nodes. Here it is very easy to see the most popular entities in the graph

- Lastly we have the “**Entity list**” – a very useful view of all entities that can be sorted by Type, Value, Incoming/Outgoing Links and entities.

- Another very cool part of Maltego is that transforms work in all views! Just try to run a transform on an entity in Entity View.



Maltego can also be used to answer some pretty complex questions, if you know how to ask them. Lets talk this one - “How can we know what websites people from Company X where looking at”? Well knowing all of the sites is going to pretty much impossible – but we could get a subset of them. If we knew all of the IP addresses belonging to a company, we could search the web for where these IPs show up – for example in publically accessible stats pages. Of course we will have a lot of False Positives here – but lets give it a go.

•I’m going to use the website of my own company TrendMicro, specifically the Irish office. But how can I get the IP address ranges used by TrendMicro? Here is a hint – many big companies will have their Mail Servers on site. So to get the IP addresses of the company, we can transform the domain Trendmicro.ie to any MX Records for that domain. Next we map these MX Records to IPs, and these IPs to a netblock (using the Whois transform). Failing that you could try the name servers, locations of websites etc until you find the right one. Alternatively you could search for emails from that company on websites instead.

•Now that we have the netblock for TrendMicro in Ireland (assuming its the only one) – lets see what sites those IPs show up on. First we expand the Netblock using “Netblock to IPs”. Next we can run the “To Website where IP appears” transform.

•Looking at the websites – some of these are obviously false positives. Click on each website and scroll down the detail view – it will give you a snippet of the site, and a link you can click on. We can delete these FPs such as www.bowdoin.edu , www.lptool.us .

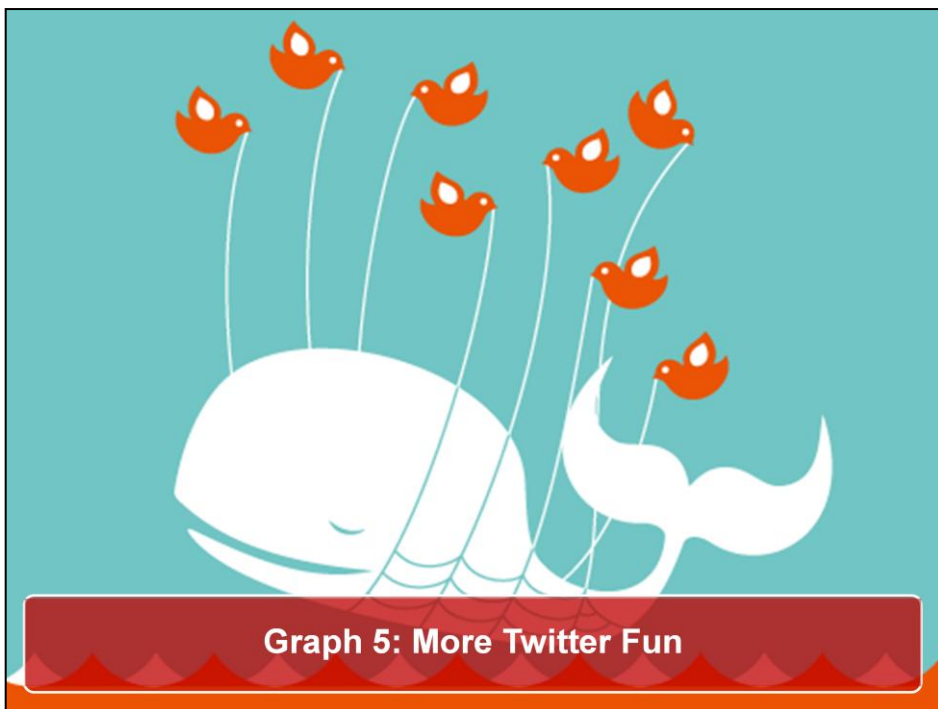
•We see a lot of sites coming from one IP in particular – a clear indication of a Web Proxy (i.e. The main point of connection for people on the network). There are some very interesting domains in here – evidence of FTP connections from 2006, and especially Wikipedia. If we visit Wikipedia we can also see more edits by the same IP address



Now every graph that we have looked at so far has been based on looking at things like Domains, Ips, Netblocks etc – but there are loads of other Entities on the internet that Maltego understands – take for instance Twitter. Twitter has a very easy to use API that lets you query all sorts of things about a twitter profile – and Maltego has some very good transforms especially for this.

So what question do we want to find out about this time? How about asking the worlds Twitter users for the best site to get information on a current topic – such as “Royal Wedding” or “Man Utd”

- Lets start with a new Entity – a Phrase. This is basically a snippet of text. Fill it with your selected topic.
- Next we are going to map this phrase to tweets that it appears in. But first we want to make sure we get as many results as possible. Do you see the “Number of Results” bar – lets set this to maximum. It has 4 settings – each limiting the number of results to 12, 50, 255 and unlimited (actually 10,000). Using the lowest setting is great for when you are poking around – but the top setting is very useful in other cases. This is one of the key differences between the Community Edition and the Commercial edition unfortunately – in the Community version this is stuck on 12. For the demo I will also use 12 – but we’ll see a full graph in a minute
- Lets transform these tweets to URLs with the “To URLs found in these Tweets” transform.
- In addition while this is still running I am going to queue up another Transform – lets extract the Hash tags from these tweets as well to see if anything interesting shows up. This is very useful as you can queue several transforms and come back when they are finished.
- Heres another useful little trick – when dealing with bigger graphs, having Maltego draw every update as it generates them can be a bit intensive of your machine. To speed things up you can **Freeze** the graph – and unfreeze it later on. To do this click the Blue Freeze button on top of the main pane. When updates have been made the button beside this will change colour, and you can click it to update the graph. You can also unfreeze everything by selecting the Freeze button.



Just for fun – and also to show the scale that Maltego graphs can expand to – I decided to set my poor 3GB laptop a challenge – “Find the most popular Security guys to follow”.

But how to go about doing that? Well I decided to start with a small Security List on Twitter, which focused on some of the Irish Security folks. Next I added these folks to Maltego. I then slammed the slider all the way to full and asked Maltego to find all of the people that they were following. This led to the pretty substantial graph at **Twitter_Twits_Stage1.mtgx**

Not content with this – I decided to go one higher! I selected all of these new people, and ran the exact same transform – resulting in the huge **Twitter_Twits_Stage2.mtgx**. This graph has over 9000 entities

How we can sort this in Entity View, or Dynamic View to get a snapshot of the Irish Security Twitter sphere!



One thing a lot of people do not realise about Maltego, is that it is actually really useful – even when you are not using any Transforms.

Maltego also gives us the ability to create our own links, without any need of transforms. This can be really useful – as you can still use all of Maltego various views to look at the data.

Here's a good example that I created earlier this year. Myself and some friends were emailing each other to see what security conferences we all planned on attending in 2011. I initially saved the results in an Excel file, but as the number of responders got bigger the spreadsheet got messier – so just for fun I decided to use Maltego.

One really good feature of Maltego is the ability to cut and paste text from the clipboard into Maltego, and it will create an Entity for it. It also does its best to guess the entity type. E.g. If you paste in 127.0.0.1 it will create an IP entity. Sometimes you will paste in something, and it will get misrecognised as another entity type – e.g. "Chaos Computer Club" is recognised as a Person not a Phrase.

If we want to be specific when we are cutting and pasting we can add the Maltego type to the text we are pasting e.g. `maltego.Phrase#CHAOS COMPUTER CLUB`

With this in mind – I pasted in all of the People, and all of the conferences. To create a link between the two simply unselect all entities, then right click drag a line from one entity to another. This will also let you add labels to the links e.g. "Definitely going", "Maybe going", etc – and change the style. If you do not care about labels, you can select the "Do not show this dialog again" button. This can always be turned back on under the Maltego Option in the main menu

So there you go – now you can draw your own graphs!



You may have noticed that I appear to have some transforms and entities in my version of Maltego that are not present in the versions you are using. There is a very simple reason for this.

Maltego was designed to be easy for anyone in the world to extend. Anyone can easily create new Transforms or Entities and publish them for others to use. Getting these new plugins could not be easier. First click the Manage tab at the top of the Window.

Lets start of by finding some new Transforms. You can easily import new Transforms for Maltego if someone provides you with a **Seed server** to sync up from. For this example we are going to use <https://cetas.paterva.com/TDS/runner/showseed/builtWith> to discover transforms that work with Builtwith.com – this is a site that shows what technologies are running on a certain domain. Thats not particularly useful on its own – but really useful if you want to see all of the technologies used by a certain company. They can also show anomalies – which might be development machines

To import these transforms select “Discover Transforms”, add that seed, and follow the wizard. We will also need to add the entities created for those transforms – you can download them from <http://ctas.paterva.com/TDSTransforms/BuiltWith/BuiltWithTechnology.mtz> and import them. On the left are options to import and Manage Entities. Here we can also create new Entities – but we will come back to that in a minute.

For a quick test I select **gov.ie** . In order to get the various subdomains like www.gov.ie, etc, I set my slider to 255 and run the DNS From Domain->To Website DNS [Using search Engine]. This searches the web for gov.ie and parses out subdomains.

To use the Builtwith API we run the ToServerTechnologiesWebsite transform. Once that is done we can use the different views to explore.

There are other transform servers – and I’ll add links at the end of these notes

Local Transforms

- Pros
 - Local Machine -> Fast to setup
 - Private
- Cons
 - A pain to share them / update
 - Everyone needs the same environment

Transform Distribution Server

- Pros
 - Much easier to share / update
 - Beneficial to the whole community
- Cons
 - Public (ish)
 - Need to setup Webservers

Create your own transforms

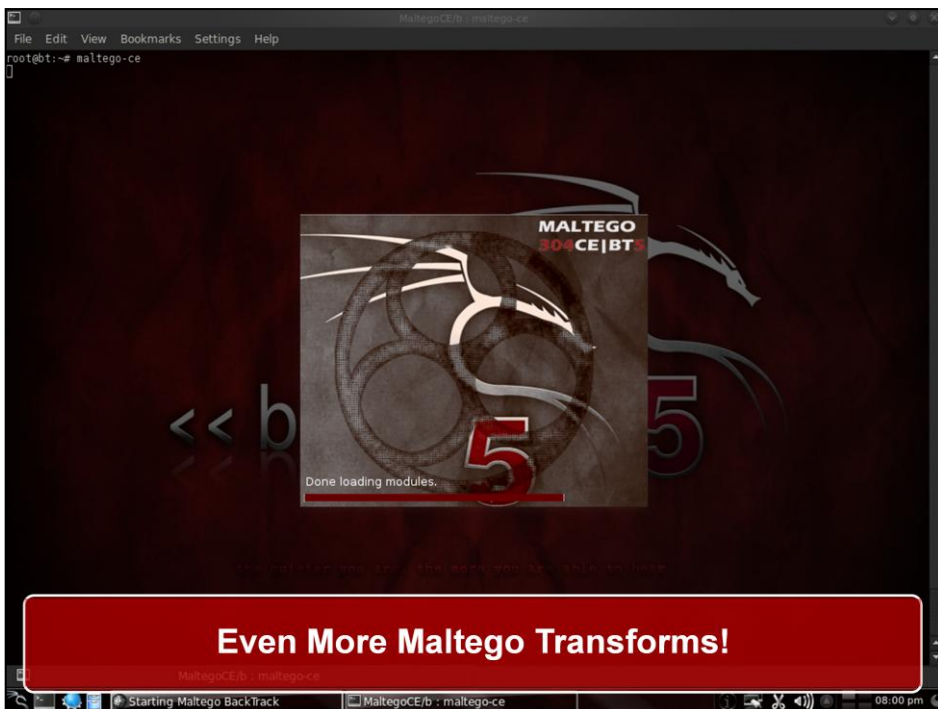
While downloading Transforms others have created can be great – often there simply is not a transform available for the job you have at hand. Perhaps its a transform for a site you always use, or even some internal web application in your company. Luckily developing your own transforms is really easy to do.

There are two main ways of developing your own transforms – you can either create them locally on your own machine, or you can create them on Paterva's Transform Distribution Servers. Both of these have pros and cons as seen on the slide. In the case of the local transforms these run directly on your machine, the TDS ones will contact the Paterva servers – which pass the information to your Web Server which works out the results and passes them back. TDS is great as you can create multiple Transforms and create your own seed to share with friends. These seeds use custom / random names – so in theory they are not public.

Paterva have given out a lot of resources to help develop your own transforms – they have created libraries in PHP and Python, detailed documentation and have an excellent support forum where people can publish their own transforms. For you Ruby programmers out there I have also ported the library across so there is also a Ruby library.

I'm conscious that not everyone in the room is a programmer, or interested in developing their own transforms – and to be honest we could have an entire workshop just on this subject (in fact Paterva did during Blackhat Europe this year) – but what I do want you to take from this is that you can easily create your own transforms (in just about any language). In the notes I'll include plenty of links to get you started.

Just to show how easy it is – we will do one last demo where I will code up a local transform, import it into Maltego and run it. But before we do that – lets look at some of the other Transforms people have made available on the forums etc



Maltego has been included in the Backtrack Linux pentesting distro for some time now, and is also in version 5 of the OS which was released this week. As well as all of the normal transforms –they have included transforms for launching Nmap scans, and also for importing network captures from Aircrack (Wifi) and mapping out the various clients, Access points etc. Paterva have also made these available on the forums on the main site. If you use either Nmap or Aircrack regularly, I definitely recommend checking these out.

Links

Facebook Transforms:

<http://www.paterva.com/forum//index.php/topic,167.0.html>

NMAP Transforms:

<http://www.paterva.com/forum//index.php/topic,134.0.html>

Airgraph-NG Transforms:

<http://www.paterva.com/forum//index.php/topic,161.0.html>



In addition to the Nmap and Aircrack transforms – no tool today would be complete without some way to integrate with Facebook. Paterva originally had some excellent Facebook transforms – mapping friends, searching Facebook for emails, phrase etc. Unfortunately Facebook do not like people scraping content from their site – and have sent a Cease and Desist letter to anyone trying to do so.

Luckily however – one enterprising member of the maltego forums (in no way linked to Paterva), has taken the time to code up his own transforms and share them with the community. They take a bit of setup time (the downside to all Local Transforms) – but once you have them up and running they do an excellent job

Also for anyone who has a lot of internal SQL database – Paterva offers solutions that will really help here.

Links

Facebook Transforms:

<http://www.paterva.com/forum//index.php/topic,167.0.html>

NMAP Transforms:

<http://www.paterva.com/forum//index.php/topic,134.0.html>

Airgraph-NG Transforms:

<http://www.paterva.com/forum//index.php/topic,161.0.html>



So just before we wrap up, I'm going to show you how easy it is to quickly develop our own transform.

For this case I am going to take the site <http://global.sitesafety.trendmicro.com> . This is Trend Micro's site to show if a website is known to be malicious or not. Wouldn't it be great to have a transform that can easily check that! So let create one.

When we use the site we notice that we put the website into the search field and press "Check it". If the site is ok the next page will have a Safe Icon, if its Malicious a dangerous icon. I'll show you a small piece of code to automate this (**trendmicro_rep_check.rb**). This code uses the Ruby Maltego API and as you can see is fairly straightforward.

To add this Transform we go to Manage->New Transform, and fill in the various fields with Entity Type set to "Website". On the next screen I set the fields as follows:

- Command: `c:\Ruby\bin\ruby.exe`
- Parameters: `c:\maltego_transforms\trendmicro_rep_check.rb` (or wherever you stored the script)
- Working Directory: `c:\maltego_transforms`

And that's it – as simple as that to create a Transform of your own



 robertmcardle@gmail.com

 www.linkedin.com/in/robertmcardle

 www.twitter.com/bobmcardle

 robertmcardle.blogspot.com



Contact Me (Please. I need friends ☹)

Just to finish up – here are my contact details in case anyone should want to get in touch.

In particular jot down the blogspot page – I'll put up a link to the notes of this workshop there tomorrow.

Overall I hope you have enjoyed the workshop, and go on to use Maltego as often in your roles as I do in mine!



Additional Resources

Transform Seeds

BuiltWith - <https://cetas.paterva.com/TDS/runner/showseed/builtWith>

SocialMedia -

<https://cetas.paterva.com/TDS/runner/showseed/SocialMedia>

Infrastructure -

<https://cetas.paterva.com/TDS/runner/showseed/Infrastructure>

Shodan - <https://cetas.paterva.com/TDS/runner/showseed/shodan>

Entities

BuiltWith -

<http://ctas.paterva.com/TDSTransforms/BuiltWith/BuiltWithTechnology.mtz>

SocialMedia -

<http://ctas.paterva.com/TDSTransforms/GraphAPI/facebookObject.mtz>

Shodan - http://maltego.shodanhq.com/downloads/shodan_entities.mtz

(check <http://maltego.shodanhq.com/>)

User Guides -

<http://www.paterva.com/web5/documentation/userguide.php>

Forum - <http://www.paterva.com/forum>

Blog - <http://maltego.blogspot.com/>

Local Transforms

PHP / Python Libraries -

<http://www.paterva.com/web5/general/resources.php>

Ruby Library - <http://www.paterva.com/forum/index.php/topic,210.0.html>

Documentation -

<http://www.paterva.com/web5/documentation/localtransforms.php>

Transform Distribution Server Transforms

Documentation - <http://www.paterva.com/web5/TDS/index.php>