

# Cork | Sec #1

18:30-19:30 Socialising ☺

19:30-20:15 Talk

20:15-??? More Socialising

SSID: FreeWifiAskServerVIP =  
sohowifi

corksec.robertmcardle.com

Hi Everyone and thanks for coming to the first version of Cork|Sec, and one that will hopefully be the first of many

I put this group together because we have quite a few Security companies around Cork at the moment, and even more people who are interested in the whole area of security. I wanted a place where we can get together once a month to socialise, and learn something practical and interesting at the same time. Even though the group name is Cork|Sec I'm also expecting techie projects as well as security ones to be presented over the coming months.

As I said on the forum and the website – this group was always modelled on a Defcon group (and in fact I may change the group name eventually if it takes off and Defcon ever come back to me). That means that it is open to Hackers and Security Folks alike. All backgrounds, ages and skill levels are welcome

The agenda for tonight is a bit of a standard template. Talks will kick off at 19:30 and we'll have socialising either side of that. Some nights we will have one talk, other nights two shorter ones.

There are lots of things you can talk about – so don't be afraid. Tonights talk is on OSINT, but you could just as easily talk about some security tool / how to secure a network / building your own quadcopter / social engineering / some malware – whatever you like as long as its both interesting and practical

INTRO MYSELF

# Tracking people online (101)

Bob McArdle

@BobMcArdle

Cork | Sec

In this talk I'm going to talk about tracking people online. I'd like this talk, like any talk we have in Cork|Sec to not be a lecture style high level talk – I'm going to try and make it as practical as possible so that everyone here learns something from tonight that they can apply afterwards. Also feel free to stop and ask me questions at any time. I'll also be sticking this talk and all the speaker notes up on the forum afterwards. So lets get cracking...

Nowadays we spend a lot of our time online, and how we are interacting with the web is constantly changing.



When I talk about interacting with the web I'm not referring to the devices we use, although that definitely changing in the direction of mobile devices and maybe later Augmented Reality.

And I'm not talking about the browsers people use, or what they are surfing to (in other words I'm not talking about tracking people using cookies)

- **Info we VOLUNTARILY put online**
- **Info we put online WITHOUT REALISING**
- **Info OTHERS PUT ONLINE about us**

What I'm going to talk about is three types of PUBLIC information:

- The information we voluntarily put online
- The information we put online without realising
- The information others put online about us

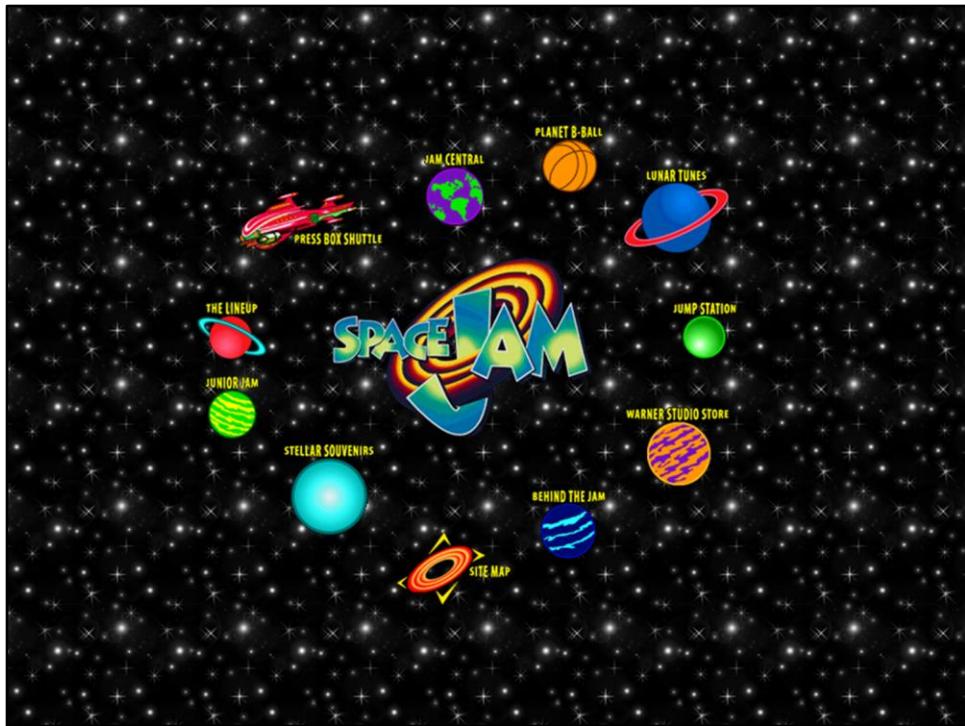
By Public I mean everything someone else could access about you without needing to discover your credentials – so I'm not talking about hacking gmail accounts, social engineering people etc – that can be a topic for another day.



Back in 2004 the buzzword Web 2.0 started to pop up a lot, and it is a bit of a buzzword – but it encompasses lots of services such as social networks, blogs, etc.

Even though it is a buzzword it does also describe a fundamental shift in how we interacted with the internet. Before Web 2.0 if you wanted to put content online you needed to be a web-designer, and understand at the very least things like HTML, Web Hosting, and if you were feeling really leet you might also know your way around JavaScript.

There are still some sites left online untouched from that era...



My favourite is the Space Jam site, which has existed unchanged since 1996.

In the interests of full disclosure my own first site was a Buffy fan-site that I put online in 1998 when I used to hang out on the old Buffy fan-forum called “The Bronze”. It was hosted with a hosting provider called 50megs.com, who where like a slightly better Geocities. It sucked, and looked awful and unfortunately (or maybe fortunately) no copies of it have survived.

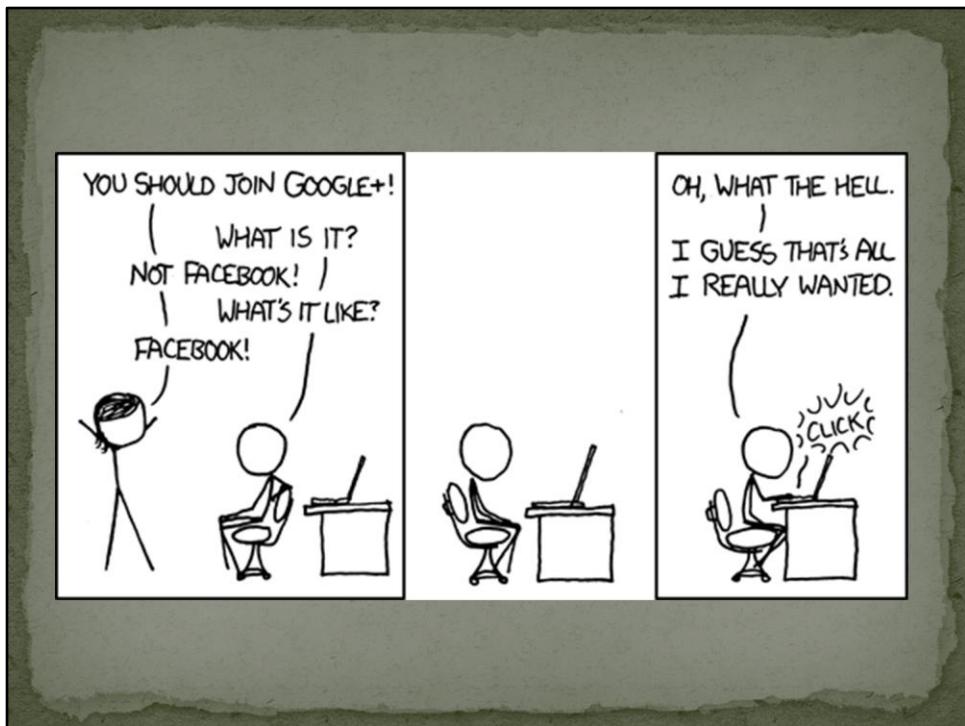
But with the arrival of sites like MySpace, Blogspot and others – everything changed. Now EVERYONE could put anything they wanted online, and that's exactly what everyone did.



Everyday mankind uploads almost 1 Exabyte of information to the web. In case you can't visualise an exabyte of the top of your head – imagine this:

If you burned all of that onto DVDs and stacked them on top of each other it would reach 4 times higher than Mt.Everest. Of course that would be a complete waste of DVDs, and everyone torrents things these days anyhow – but you get the idea. Its a LOT of data.

So lets start by looking at the channels through which people share information about themselves online, and then look at the type of information they share online – and then we'll get to the main focus of this talk – showing you ways you can track information about people.



The main channels that people PUT information online about themselves is:

Social Networks – such as LinkedIn, Facebook, Twitter and Foursquare

If you still have a MySpace account and are not in a band you're not retro, you are just horribly out of date – time to update to at least Bebo.

Talk to... Boards.ie Adverts.ie Arts Biz Edu Games Hosted Music Rec R

**BOARDS.IE**

Find forums, users and posts

Home > Tech > Security > Cork|Sec - Info Security Monthly social meetup

 Plus get 100MB data a day 

**Post Reply** **Unfollow**

16-06-2013, 16:33

**hantakage**  
Registered User  
☆  
Join Date: May 2005  
Posts: 40  
Adverts | Friends

**Cork|Sec - Info Security Monthly social meetup**

Hi Everyone

I am starting a monthly Info Security meetup in Cork. Regardless of whether you identify yourself as an InfoSec person or someone with an interest in breaking things to see how they work / stopping people breaking things to see how minded friends

For more information head on over to <http://corksec.robertmcardle.com/>. There is also a forum where you can attend please sign up to the forum because It gives us an idea of the numbers we can expect to show up. To keeps SPAM posts to other forums / address announcements of venue etc) will be only sent to forum members.

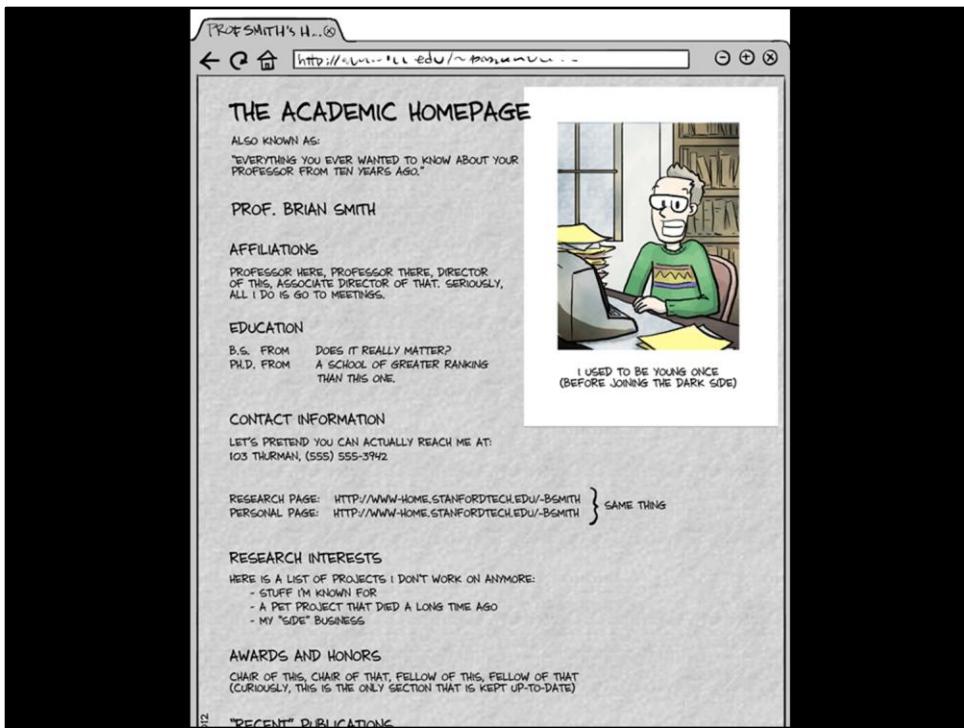
Also if you know anyone else who may be interested in this meetup - no matter what their profession or skill-level

Bob McArdle  
<http://ie.linkedin.com/in/robertmcardle>

Next there are discussions boards, IRC and IM clients



Then there are gaming sites such as Steam or World of Warcraft



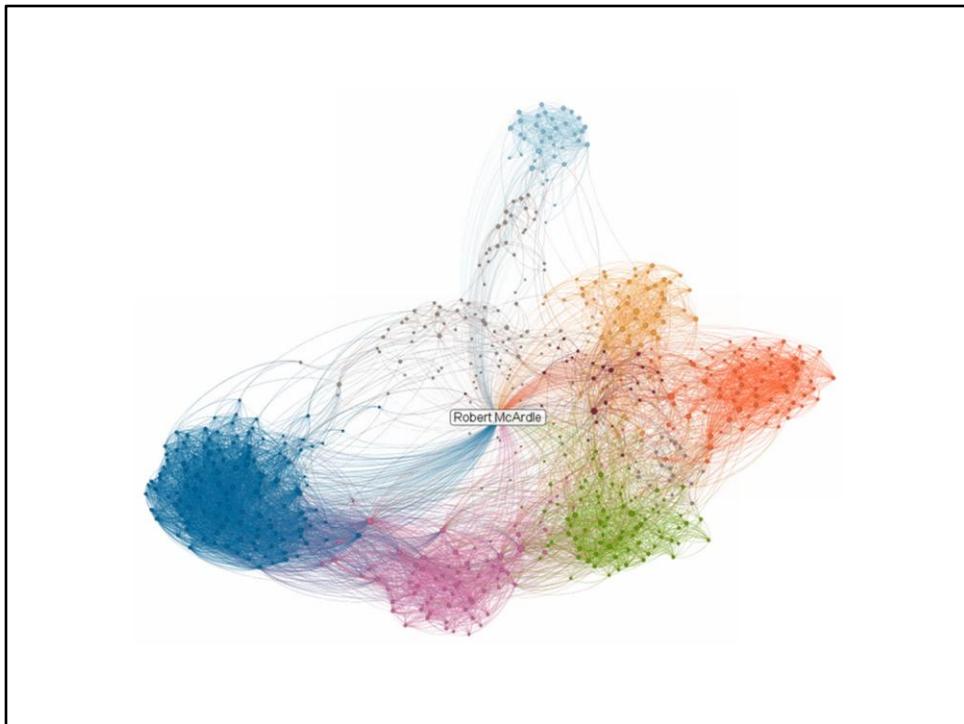
And of course personal profile or homepages – these are especially popular among members of the Academic community and creative people such as artists or designers. This category also includes dating sites.

So with all these sites – what sort of information do people publically share about themselves?

Well at a first glance we have of course peoples

- Name
- Age
- Sex and Sexuality
- Pictures
- Location
- Job
- Educational History
- Interests (including political interests)

But we can go deeper than just those details, we can look into Social Graphs



But we go deeper than those details – we can look into things like Social Graphs – to quickly see what interests a person has in common with others, who are the key influencers in groups, family connections and so on.

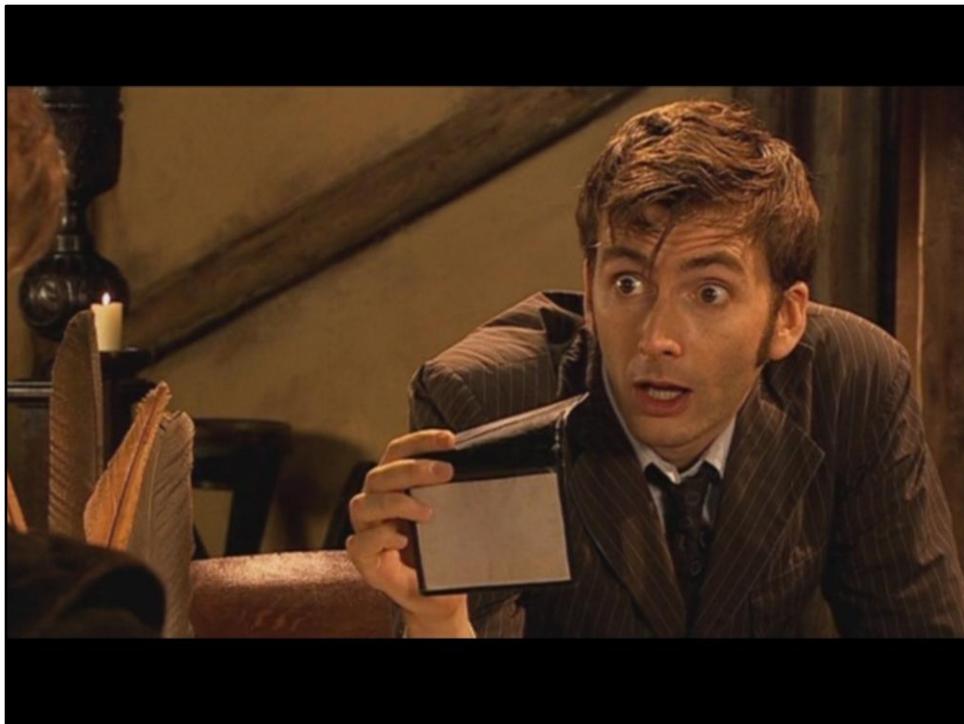
The graph on the slide is my LinkedIn network graphed out, you can see sections that split off e.g. Trend Micro employees, Security folks etc. Very nice way to see who are central to an online community.

SHOW LIVE DEMO – KEY PEOPLE IN MY NETWORK – PAUL FERGUSON, TIM HORGAN, OTHERS

But why would someone , some attacker / government / competitor etc care about all of your details?

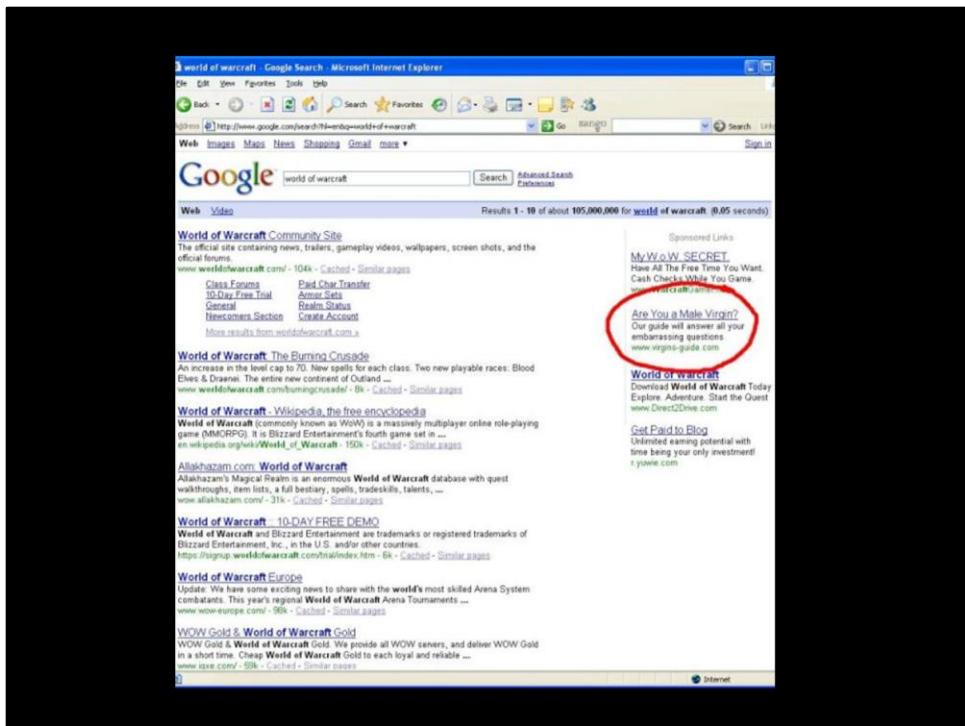
Well your identity once known is a very powerful thing...

Link: <http://inmaps.linkedinlabs.com>



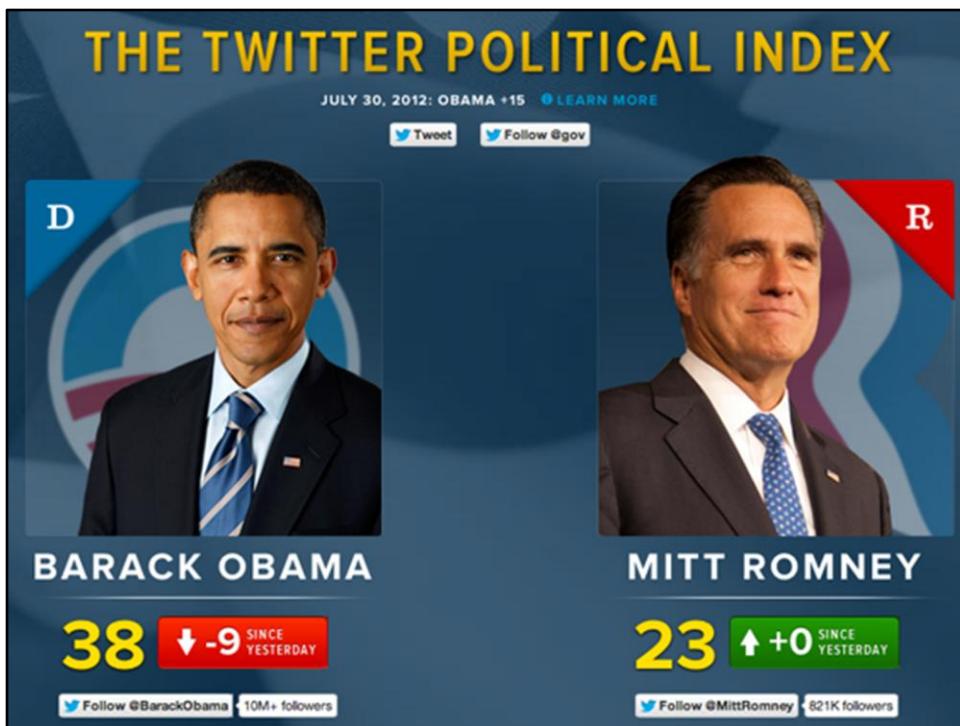
-- It can be used to impersonate you. The more details about yourself that you put online, the more information you give to scammer to pretend to be you e.g. To your bank. If a banks security check relies on knowing your DOB, pets name and mothers maiden name - a simple Facebook search will normally do the trick.

By the way for any non-Doctor Who fans – that's Psychic paper – go look it up



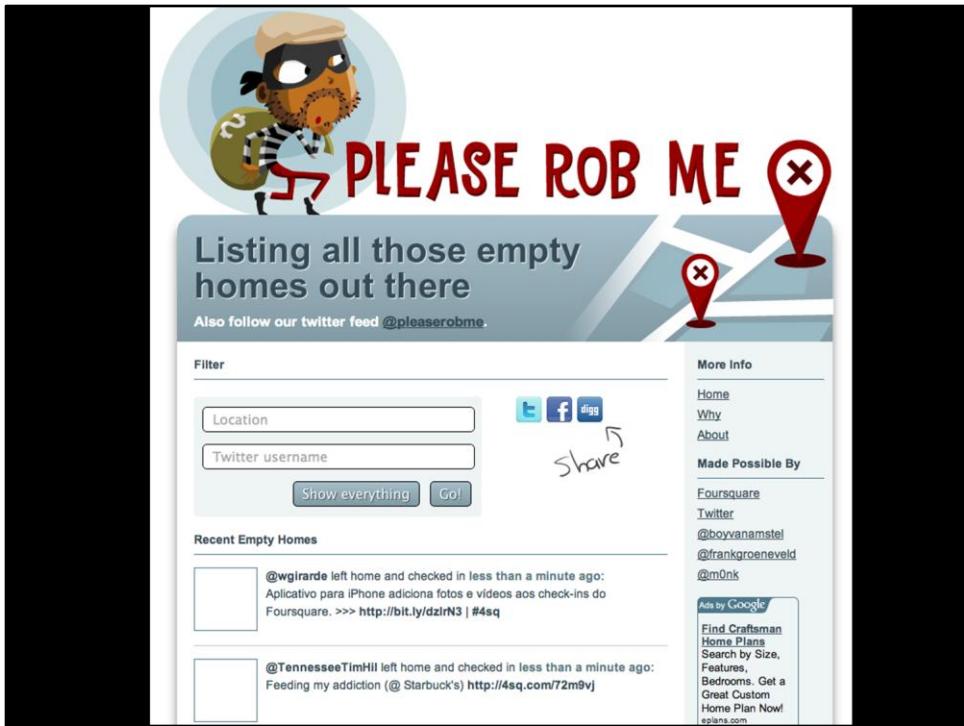
Advertisers can of course make use of your personal interests, and your social networks interests to accurately target you with ads – in order to get you to buy goods they are promoting. This whole area is REALLY fascinating and REALLY murky, but goes beyond the scope I have in mind today.

(NOTE: Sorry about all the WOW bashing ☺ )



Governments can use your data to predict voting preferences based on the language of your tweets and facebook posts, to get a better idea of discontent in the electorate or who is going to win the next election.

To paraphrase a Henry Kissinger quote that sums this up well – “Elections are far too important to be left up to the people to decide”.



And of course while knowing someones location is very powerful if you want to track someones movements, just as powerful is knowing where someone is not

An excellent example of this was the site PleaseRobMe.com which monitored Twitter for tweets about people leaving home, and correlated that data with a person home address and what they had publically bought on eBay or Amazon. Want to search for all the people in Cork who have purchased a new TV online in the last 6 months and are currently on holidays? Its pretty easy with some simple web scrapping.

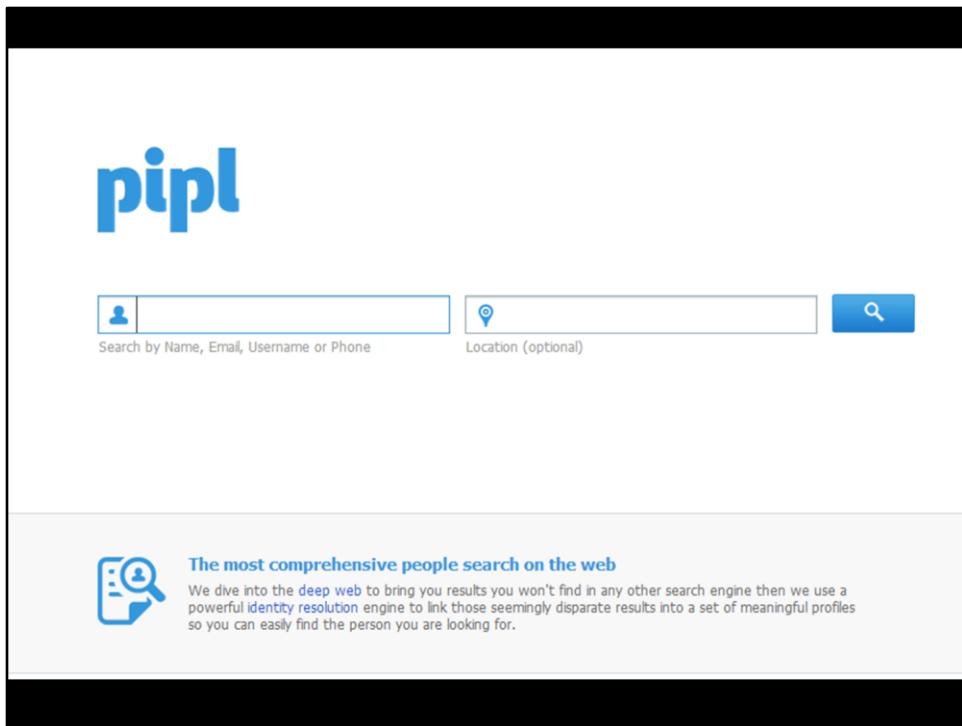
So thats an idea of why a person may want to track someone online – lets look at some real world examples of the sort of details you can find about someone online

# 1. People Search Engines

---

Cork | Sec

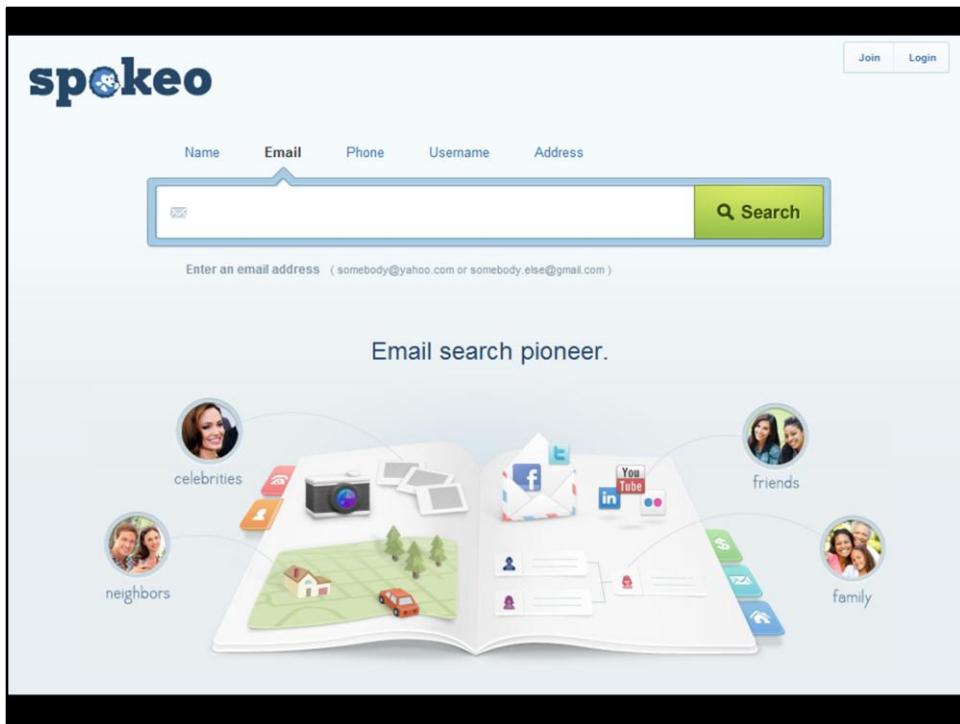
One very handy category of website for doing a first pass of the information a person has put online are “People Search Engines”



One of the most popular of these is [pipl.com](http://pipl.com)

These sites allows you to search by name, email, username or phone. In turn it will search through the so called “Deep Web”, searching sites such as Twitter, Facebook, Amazon, eBay, Picasa and a host of other sites to find profiles belonging to people with the information you provided. The success using this site will vary depending on the information you have to start with – but I have often found it to be an excellent starting point for tracking down individuals.

Links: [pipl.com](http://pipl.com)



Another site that offers a very similar service to Pipl is Spokeo.com, which is probably the most well known people search engine. There are two versions of the service – free and premium. Premium reveals even more data for a small fee. To be honest the free version keeps most of the data locked away – but if you do find yourself needing to track people online on a regular basis, getting the premium account is well worth while.

1. DEMO – PIPL: ROBERT MCARDLE, ROBERTMCARDLE@GMAIL.COM
2. Much better at getting data on Americans – Example, what can we get with just a phone number
3. Show CrimeReports.com

So overall these type of sites are good starting points to get you started into profiling someone, you still need to wade through some data – but at least you are not going over the entire internet.

Links: [Spokeo.com](http://Spokeo.com)

## 2. Social Networks

---

Cork | Sec

Next up is Social Networks. In most cases it is always a good idea to go a search for at least Facebook and LinkedIn. Both are VERY popular services. If you know however that the person you are profiling has a specific interest, or comes from a certain part of the world – that will also affect what sites you use. For example if the person was Russian you should check Vkontakte, if Brazilian Orkut and so on.

Facebook has an advanced search page that lets you search for someone by

- Where they live
- Education
- Mutual connections
- Job History

And of course name, and email if they share that

DEMO: IDF and Curragh

<https://www.facebook.com/find-friends/browser>

The screenshot shows a Facebook search interface. The main search bar at the top has the query: "Family members of people who live in China and like Falun Gong". Below the search bar, the results are displayed in a grid format. Each result card contains a small profile picture, the user's name, and their relationship status (e.g., "Sister of [redacted] likes Falun Gong"). To the right of the results, there are two sidebar sections: "REFINE THIS SEARCH" and "EXTEND THIS SEARCH".

- REFINE THIS SEARCH:** Includes dropdown menus for Gender (Add...), Relationship (Add...), Employer (Add...), Current City (Add...), Hometown (Add...), School (Add...), Friendship (Add...), and Relatives of (with a dropdown for "China residents who like Falun Gong"). There is also a "... SEE MORE" link.
- EXTEND THIS SEARCH:** Includes links for "Photos of these people", "These people's friends", "Places where they've worked", and "... SEE MORE". At the bottom, there is a "Discover Something New" button.

And Facebook is getting a LOT more powerful. They are opening up Facebook Graph Search, which up until now was internal only.

This will let you make searches on other aspects as well – such as Likes, Photos posted etc. But more importantly it lets you map relationships.

Here is a search of people living in China that have “liked” a group which the China government cracks down on.

Links: <https://www.facebook.com/about/graphsearch>

**Spouses of married people who like Ashley Madison**

Married to [REDACTED] likes Ashley Madison · [REDACTED]

Add Friend Message

Married to [REDACTED] since [REDACTED] 2010 · [REDACTED] likes Ashley Madison  
Studied at [REDACTED]

Add Friend Message

Married to [REDACTED] since 2008 · [REDACTED] likes Ashley Madison  
Studied at [REDACTED]  
Listens to [REDACTED]

Message

Married to [REDACTED] likes Ashley Madison · [REDACTED]  
Studied at [REDACTED]  
Listens to [REDACTED]  
19 followers

Gender Add...  
Relationship Add...  
Employer Add...  
Current City Add...  
Hometown Add...  
School Add...  
Friendship Add...  
Married to **Married people who lik...**

SEE MORE

Photos of these people  
These people's friends  
Places where they've worked

SEE MORE

Discover Something New

Heres one for Married People who have liked the site Ashley Madison , which is dedicated to hooking up people who want to have affairs.

More Than 100 People

REFINE THIS SEARCH

Gender: Female

Relationship: Single

Employer: Add...

Current City: Add...

Hometown: Add...

School: Add...

Friendship: Add...

Likes: Getting Drunk!

Live Near: Me

Interested In: Men

SEE MORE

EXTEND THIS SEARCH

More pages they like

Photos of these people

These people's friends

SEE MORE

And this one is pretty creepy – this was posted to the site  
<http://actualfacebookgraphsearches.tumblr.com/>

But you can see the power in something like this for zeroing in on people.

The screenshot shows the LinkedIn Advanced Search results page for the query "MARINA NUCLEON". The search bar at the top contains the term. Below it, the search filters are expanded, showing:

- Relationship:** All (selected), 1st Connections (0), 2nd Connections (0), Group Members (0), 3rd + Everyone Else (6).
- Location:** All (selected), United States (6), Baltimore, Maryland Area (2), Hawaiian Islands (1), Greater New York City A... (1), San Francisco Bay Area (1). There is also a "+ Add" button.
- Current Company:** All (selected), US Army (1), SAIC (1), L-3 National Security S... (1).

The results list shows 6 entries:

- LinkedIn Member**: Freelance DevOps Pro, Greater Seattle Area - Internet. Summary: ..., AMHS, NUCLEON, TRAFFICTHIEF, ARCMAP, SIGNAV..., BANYAN, MARINA. **Send InMail**
- LinkedIn Member**: Information Security, San Francisco Bay Area - Information Technology and Services. Summary: ...ANCHOR, AMHS, NUCLEON, TRAFFICTHIEF, ARCMAP, SIGNAV..., BANYAN or MARINA. **Send InMail**
- LinkedIn Member**: Senior Intelligence Analyst at SAIC, Baltimore, Maryland Area - Defense & Space. Specialties: ..., Fascia/Banyan, Gamut, Intelink, JWICS, Mainway, Marina, Nucleon, Octave, Plinwale, SNAPE, Synapse, UIS... **Send InMail**
- LinkedIn Member**: Intelligence Analyst at L-3 STRATIS, Hawaiian Islands - Defense & Space. Past: Intelligence Analyst at United States Air Force ...OS, M3, MAINWAY, MARINA, MAUI, MESSIAH, MICROBAS..., MIDB, NSANET, NIMBLE, NRIT, NUCLEON, OCTAVE...
- LinkedIn Member**: Analyst at 20755, Baltimore, Maryland Area - Internet. **Send InMail**

On the right side of the results, there are three ads:

- Recruiter Conference**: Expert speakers, leadership development, & more. Sept 15-18 in Sonoma, CA.
- Accounting MBA - Online**: Earn a consistently Top Ranked MBA - 100% online with tracks in Accounting.
- Earn an MBA in 12 Months**: Program Length May Vary. Study & Earn Your MBA Online. Learn More Today!

Then we have LinkedIn. Its Advanced Search page is very powerful. With this you can find profiles based on a wide range of information:

Location

Any current / previous job

Any current / previous education

Seniority

Language

Interests

And of course keywords – here MARINA and NUCLEON are two NSA programmes disclosed by Edward Snowden...

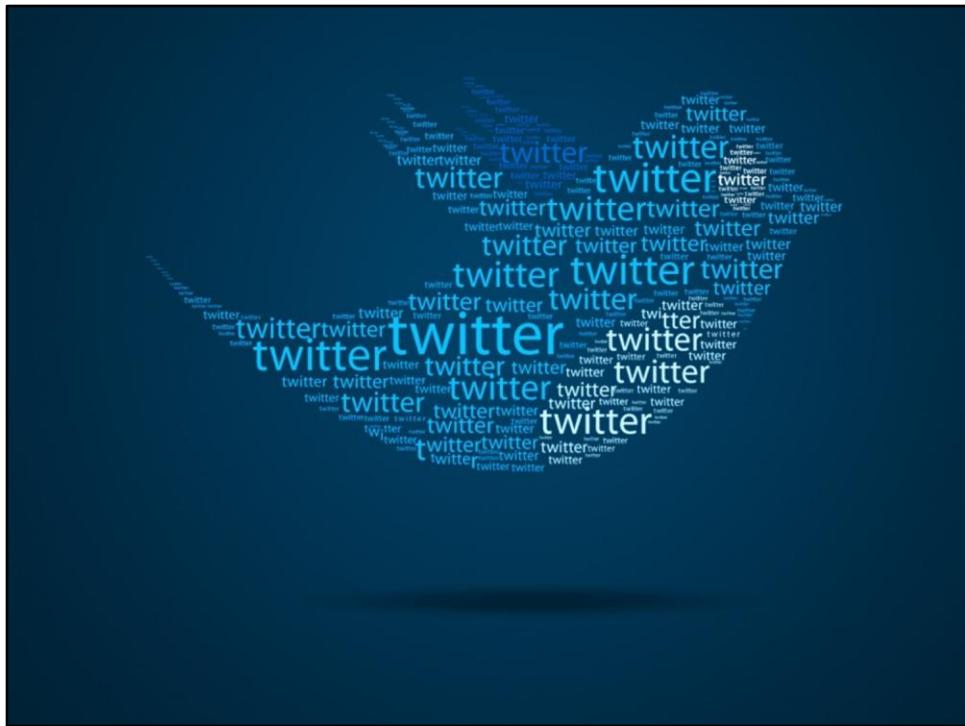
... And heres a profile that gives us a bunch more

People often reveal FAR too much info in a linkedIn profile. For example if someone posts that they work at a company and have experience with

Windows Admin  
 Checkpoint Firewall  
 Symantec AV

Congratulations – you just described your corporate network to an attacker and he did not even need to scan it 😊

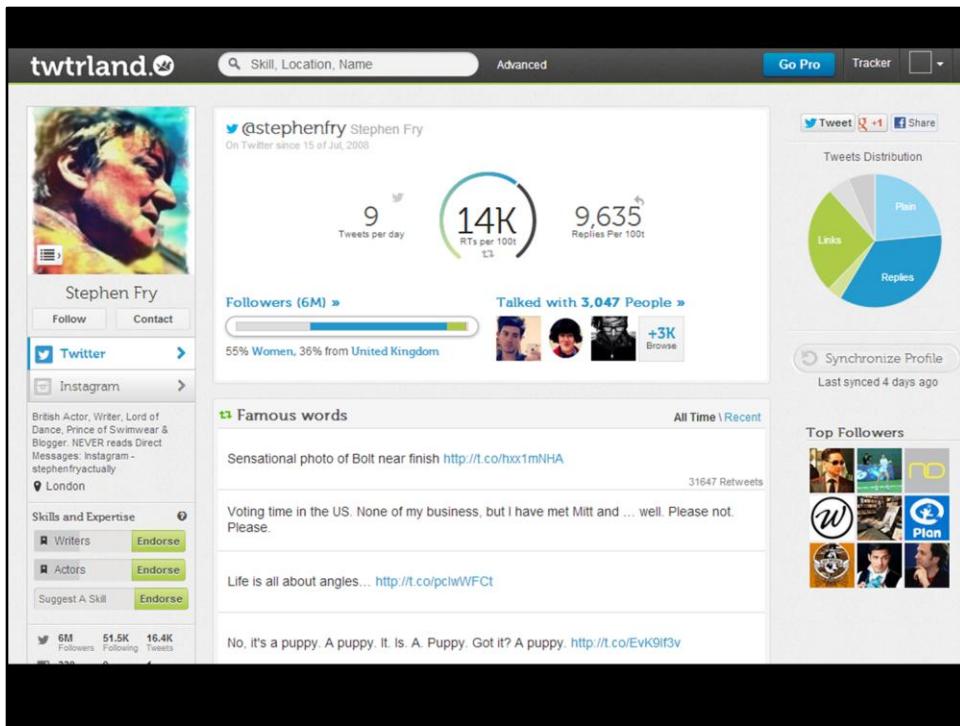
One careful thing to note here – you normally need to be logged into LinkedIn to do any sort of advanced searching BUT everything you view someones profile it will be shown to the person that you viewed them. The lesson here is – set up a dummy account.



Probably my favourite Social Network for this type of thing however is Twitter. Twitter is a gold mine of information!

One of the big differences between Twitter and Facebook is that by default all tweets are fully public. In one sense that's pretty similar to Facebook, but in general a lot more people have started to lock down their Facebook account but think nothing of posting all sorts of useful details to twitter.

Twitter also has a very thorough API that allows you to interact with it quite easily, and which has lead to an abundance of free tools for monitoring peoples activities. Unfortunately this API has recently undergone a major update that has broken a lot of the best tools 😞



Lets start by looking at Twtrland.com. This is a really useful site that give lots of statistical breakdown on a person, and can help to gain insight into their interests, friends and so on

#### DEMO – BOBMCARDLE

- Show the Followers Breakdown
- Show the conversation breakdown
- Tweets distribution shows what they use Twitter for e.g Bobmcardle mostly sharing links and RT, not that personal
- Audience Demographics give a hint to location
- Skills plus followers skills indicate interests
- Can also see all tweets mentioning me
- Can go to Twitter Advanced Search to see conversations

Links:

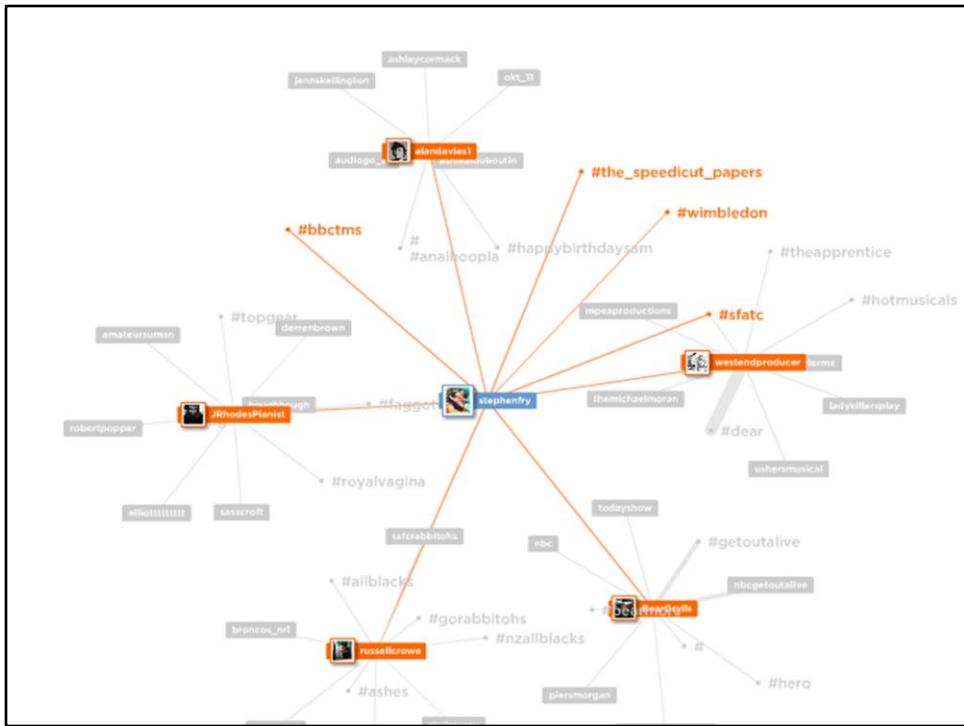
twtrland.com

<https://twitter.com/search-advanced>



Another very simply Twitter App for getting an idea where someone lives is SleepingTime. Simply by graphing out peoples tweet times it can find out when they are likely to be awake . Police can make use of this for planning arrests.

Link: <http://sleepingtime.org>



For visualising Twitter relationships a handy site to use is MentionMapp

This site will take a profile and build a map based on the people and hashtags that person has mentioned most in most recent tweets

## DEMO

Links: <http://mentionmapp.com>



No talk on OSINT or tracking people would be complete without mentioning the phenomenal Maltego. If you only remember one tool from tonight this is definitely the one to remember.

Maltego has a whole range of uses, many of them for profiling networks – but it is also very strong on the person front also.

Lets look at Some twitter related DEMOs

DEMO – Paris Hilton location check based on Images posted

DEMO – Relationship between two people

-- Get who follows them

-- Then who they follow

-- Pick the ones with 4 links and copy to new graph with 1 parent

### 3. Online Discussions

---

Cork | Sec

As well as social networks – online discussion forums can be very useful for profiling a person. These are often going to be country or interest specific.

Talk to... Boards.ie Adverts.ie Arts Biz Edu Games Hosted Music Rec Region Science Soc Sports Tech

**BOARDS.IE** Find forums, users and posts 

Currently active users: 6,491 (2,288 registered, 4,203 guests)

**DOWNLOAD OUR APP**  
AND GET BROWSING IN SECONDS  

Latest Posts My Forums My Threads Trending Thanks

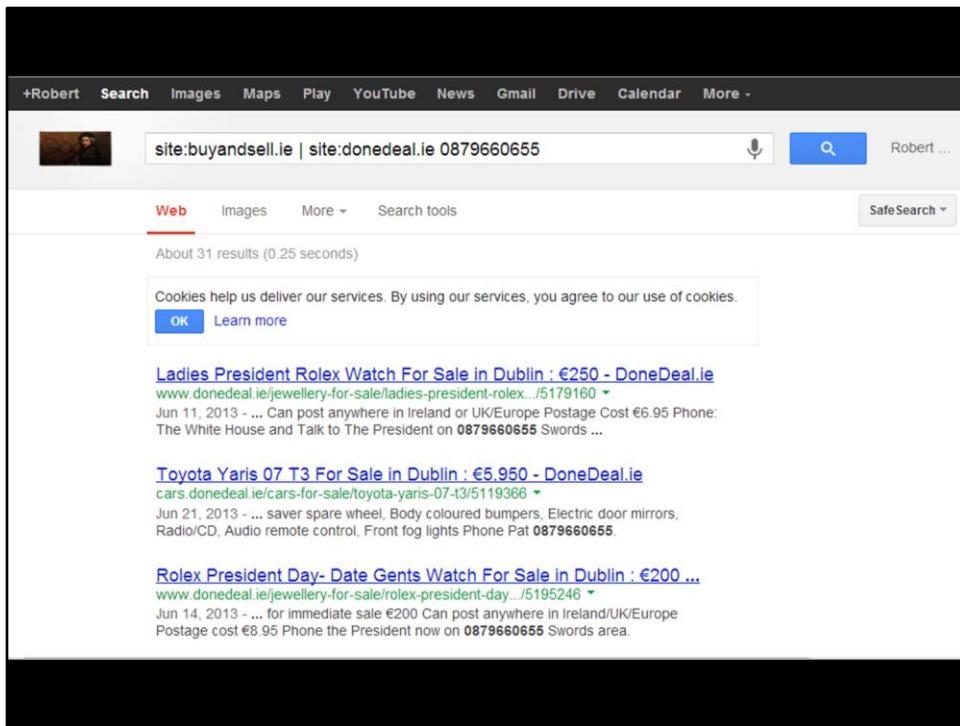
Latest Posts		All Topics	
Motors   Advice re a car accident please!	32 Posts	8 Thanks	
15-Jul 22:30   Latest post by Kenny_Loginis			
After Hours   Dumb/Great Facebook Status {merge} [No Names]	4,936 Posts	25,833 Thanks	
15-Jul 22:30   Latest post by coolhull			
After Hours   ALLEGED FINE GAEL SEX PROBE	3 Posts	0 Thanks	
15-Jul 22:30   Latest post by SamHall			
After Hours   prialtebay blocked	14 Posts	1 Thank	
15-Jul 22:30   Latest post by Chucken			
After Hours   Zimmerman trial verdict predictions	421 Posts	247 Thanks	

Announcements  Have you seen our new About Us?

[View all announcements](#)

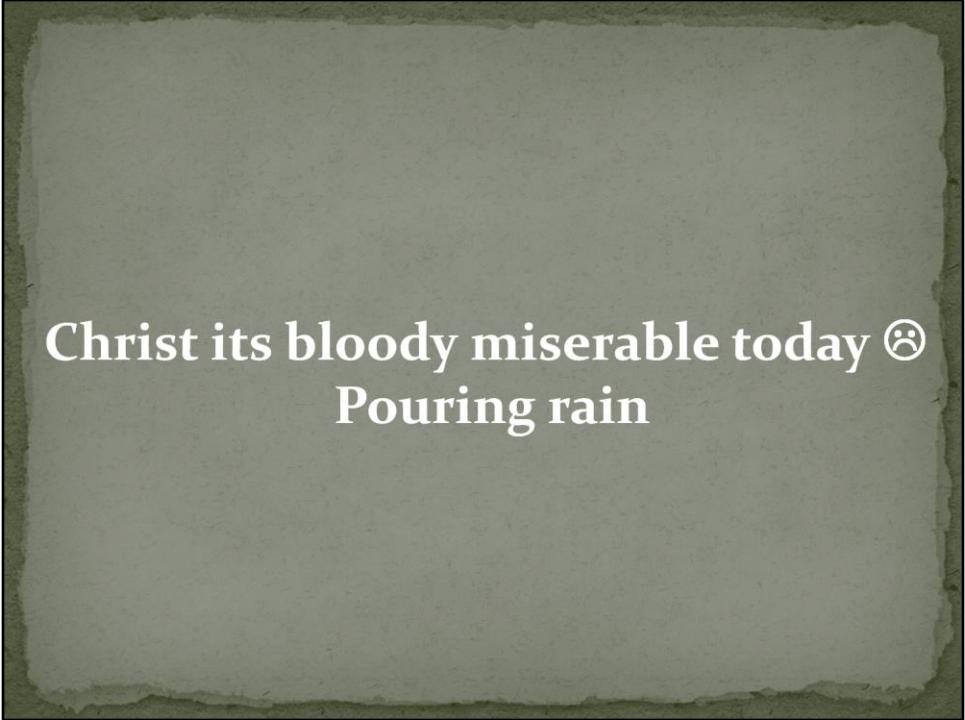
**GET ALL THE ANSWERS**  
in one place, straight from the source

So for example if your target was in Ireland, boards.ie is a very useful site. Or if you knew your target was interested in soccer I would check the various sporting forums and fantasy football sites.



Classified ads are also a very useful site for finding people . In the US craigslist is king, but over here its DoneDeal and BuyAndSell. Using a simple google dork you can easily search for posts containing certain keywords or phonenumbers for example.

By the way this is a very useful search if you ever have your house burgled. Make a list of unique items that were taken and search for them to see if someone sells them. You'd be surprised.

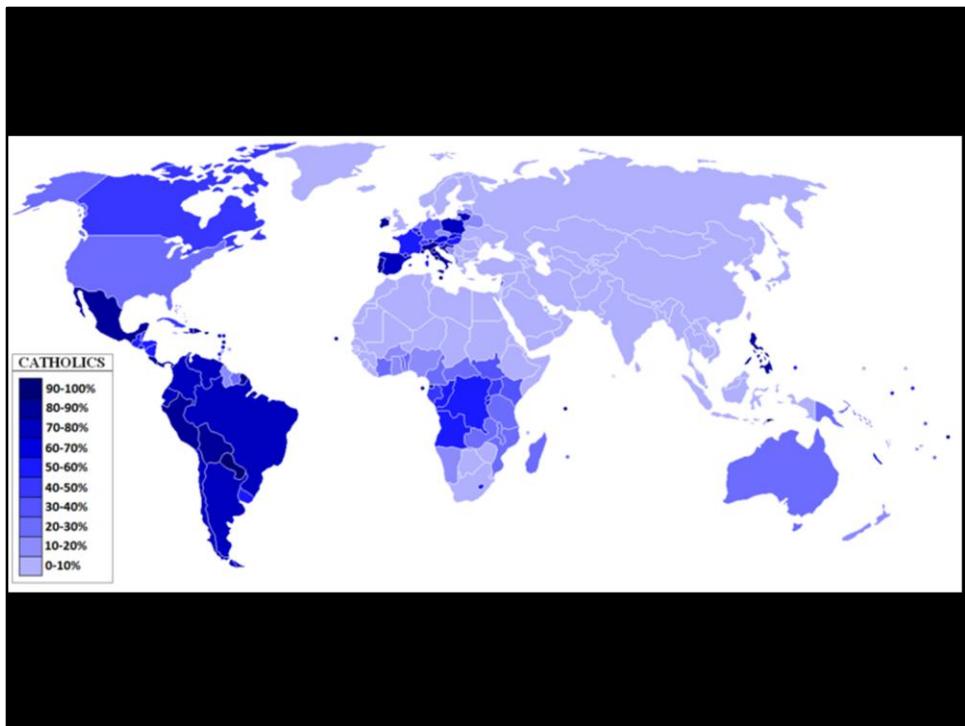


**Christ its bloody miserable today ☹  
Pouring rain**

Sometimes it's what people reveal without realising it which is the most interesting thing when it comes to discussion forums.

Take this line for example, from an IRC log. Seems innocent enough, but what can these 7 words tell us about the writer.

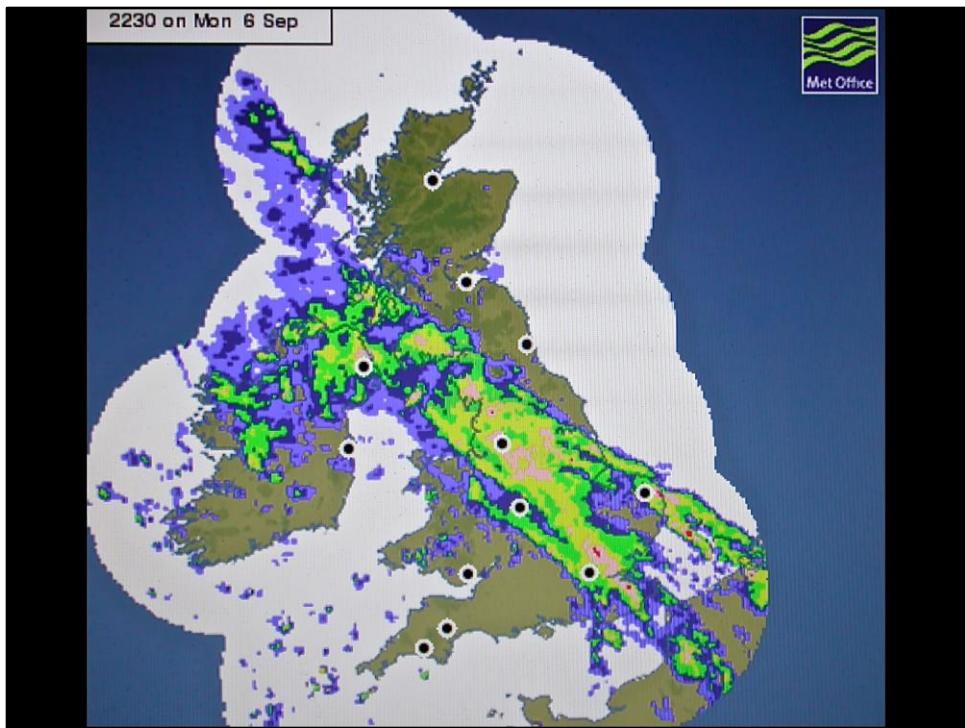
Well to start with this could have been written by any of the 7 Billion people on the planet, but only 2.4 Billion of those use the internet – so that's a start.



Then there is that first word – Christ. That indicates that the person who is writing is a Catholic. A breakdown of the world's religion now places the person most likely in Europe, South America or the US

But the use of slang and short sentences would indicate this is a natural English speaker – that narrows us down (most likely) to the US or Ireland and possibly England.

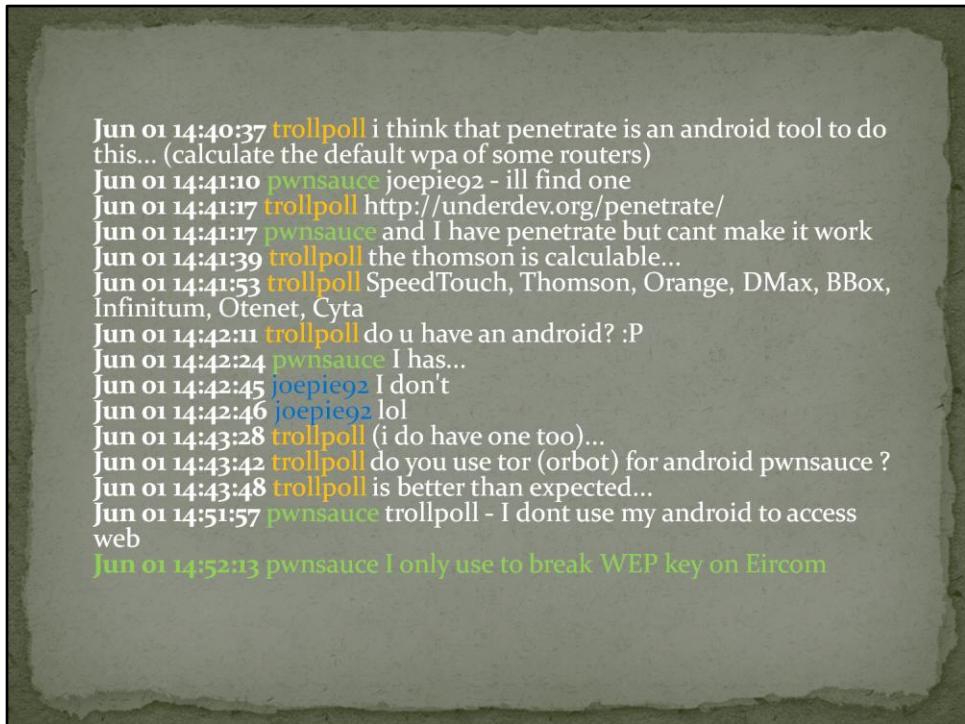
Then there is the use of the word Bloody – that is much more popular in England and Ireland than in the other two.



Even the weather gives a clue. If we assume the person is in the British Isles we can now narrow them down to the areas with high rainfall at the time the post was made. The fact that the person is talking about the weather also can give you an indication that it is daytime where they are – people tend to only complain about weather when they can see it – so that means its daytime and they are near a window.

Thats a lot better area to start searching than the 7 Billion people we started with – and that was just one line. Every line can potentially reveal something.

And stuff like this does happen in real life – take this example:



This was one of the leaked IRC chats from Anonymous – notice the last line. Thats a pretty big #FAIL and narrows the user down quite a lot

From that we can see that PwnSauce owns an Android phone, lives in Ireland and was most likely logged into Eircom at the time shown.

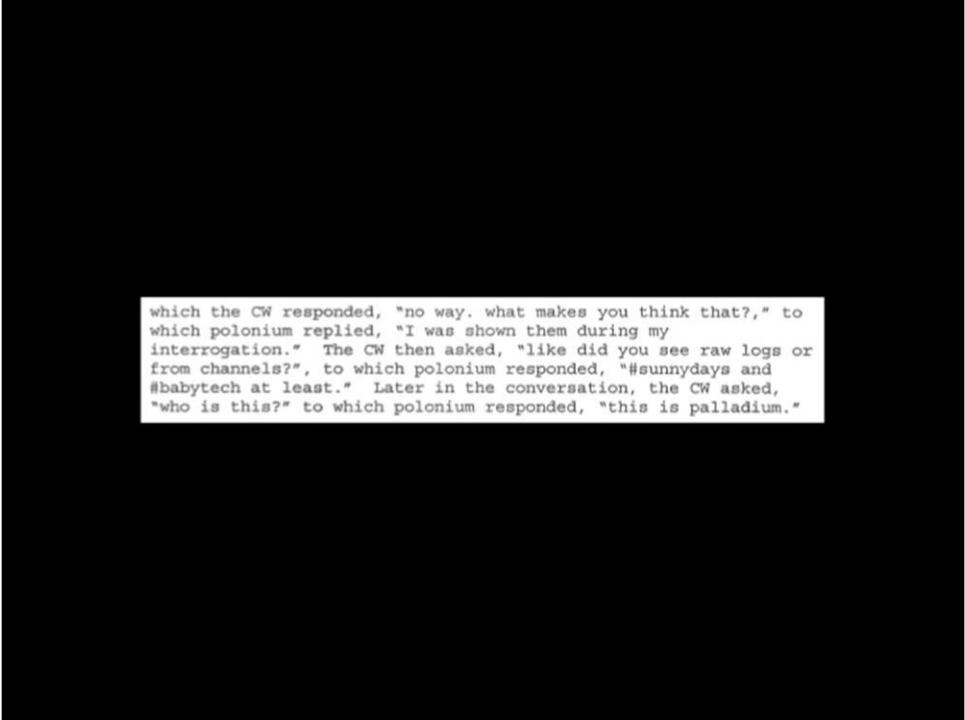
In fact Lulzsec seem to have made all sorts of messups in their OpSec when it comes to posting online. Based on the public FBI arrest details – there are all sorts of details...

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "~~arrested for weed and did two weeks in county jail.~~" Later in that same chat that individual said: "~~Don't tell anybody cause it could compromise my identity but I am on probation . . . I've done time before though it's all cool.~~" In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

(b) (6) (A) (ii) (B) (6) (C) (4) (D) (6) (E) (6) (F) (6) (G) (6) (H) (6) (I) (6) (J) (6) (K) (6) (L) (6) (M) (6) (N) (6) (O) (6) (P) (6) (Q) (6) (R) (6) (S) (6) (T) (6) (U) (6) (V) (6) (W) (6) (X) (6) (Y) (6) (Z)

Here one suspect narrows his identity down nicely for police to those people in the US who have done 2 weeks prison sentence for weed and are currently on probation.

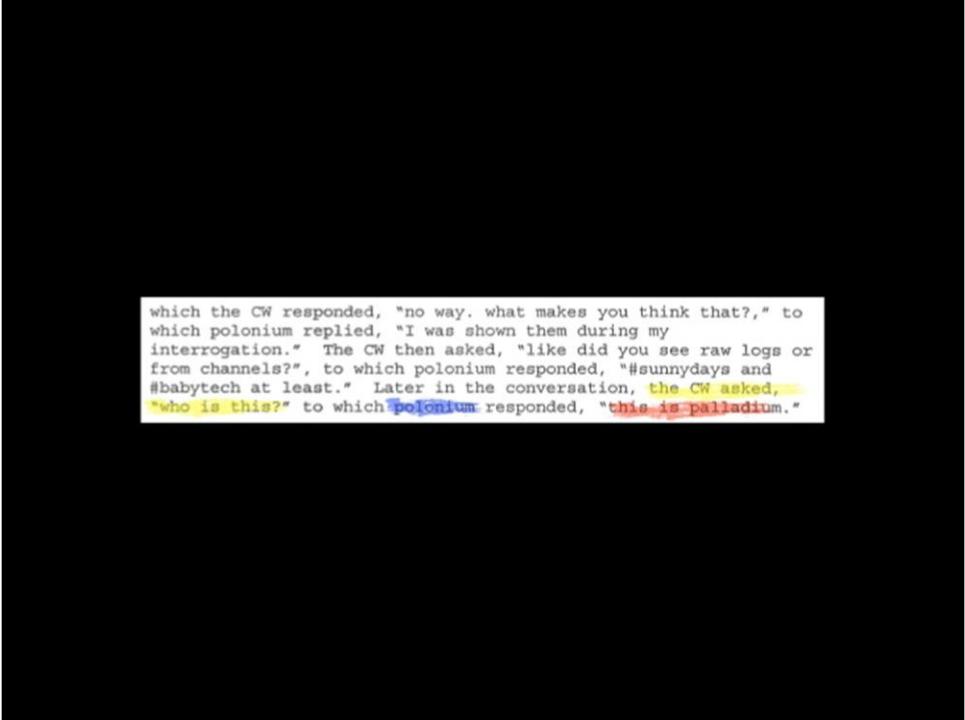
Src: <http://www.slideshare.net/grugg/opsec-for-hackers>



which the CW responded, "no way. what makes you think that?", to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #bytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

Our own fellow country men where at it also – can you spot what is wrong with this one?

Src: <http://www.slideshare.net/grugg/opsec-for-hackers>



which the CW responded, "no way. what makes you think that?", to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #bytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

I love when someone I'm tracking does this. In one simple sentence the person has linked together two of their online nicknames – this makes it MUCH easier for an investigator to then correlate the data they know about one nickname to what they know about the other one – actually reducing the amount of data to go through.

Src: <http://www.slideshare.net/grugg/opsec-for-hackers>

know that on or about January 9, 2012, the CW and anonsacco exchanged Internet chat messages . During the chat, anonsacco stated, "I just got into the iCloud for the head of a national police cybercrime unit. I have all his contacts and can track his location 24/7."<sup>10</sup> Anonsacco then referenced "sunnydays", after which the CW inquired, "so who were you? if you know about !sunnydays," and "the channel name was leaked to feds. so clearly im interested in who you were," to which anonsacco responded, "I understand it was leaked. That caused me a lot of hassle. Could you understand that I don't want to align myself with a compromised screenname?" The CW then asked, "hassle how? you got raided? or people doxed<sup>[11]</sup> you?" Later, the CW asked, "so if you were raided, did they ask you about me?", to which anonsacco responded, "No. Not you personally."

To be fair – he did learn his lesson after the first time.

Src: <http://www.slideshare.net/grugg/opsec-for-hackers>

The screenshot shows the homepage of KnowEm. At the top, there's a navigation bar with links for "Check Username", "Create Profile", "Community", "Networks", and "About". On the right side of the header, there are fields for "username" and "password" with a "SIGN IN" button, a "Remember me" checkbox, and a "SIGN UP" button. To the right of these, there's a yellow call-to-action button that says "RESERVE YOUR NAME ON HUNDREDS OF SITES CLICK HERE". Below the header, there's a large orange arrow pointing down towards a search input field. The search input field has the placeholder text "enter name here" and a yellow "Check It" button next to it. To the right of the search area, there's a section titled "What is this?" which describes the service: "KnowEm allows you to check for the use of your brand, product, personal name or username instantly on over 550 popular and emerging social media websites. Grab your name and secure your brand before someone else does." Below this text is a "Learn more" link. Further down, there's a section titled "KnowEm for the Enterprise" with a "KnowEm Enterprise Dashboard" button. At the bottom of the page, there's a grid of various social media and website logos, including StumbleUpon, Twitter, Blogger, FriendFeed, tumblr., Behance, Facebook, Squidoo, Kiva, Fiverr, issuu, pen.io, tinychat, foursquare, Delicious, TypePad, USTREAM.TV, Pinterest, Vimeo, Etsy, Alltop, folkd.com, LinkedIn, and uservoice.

If you want to know what sites a person may be on, and have their username – I definitely recommend giving KnowEm a try

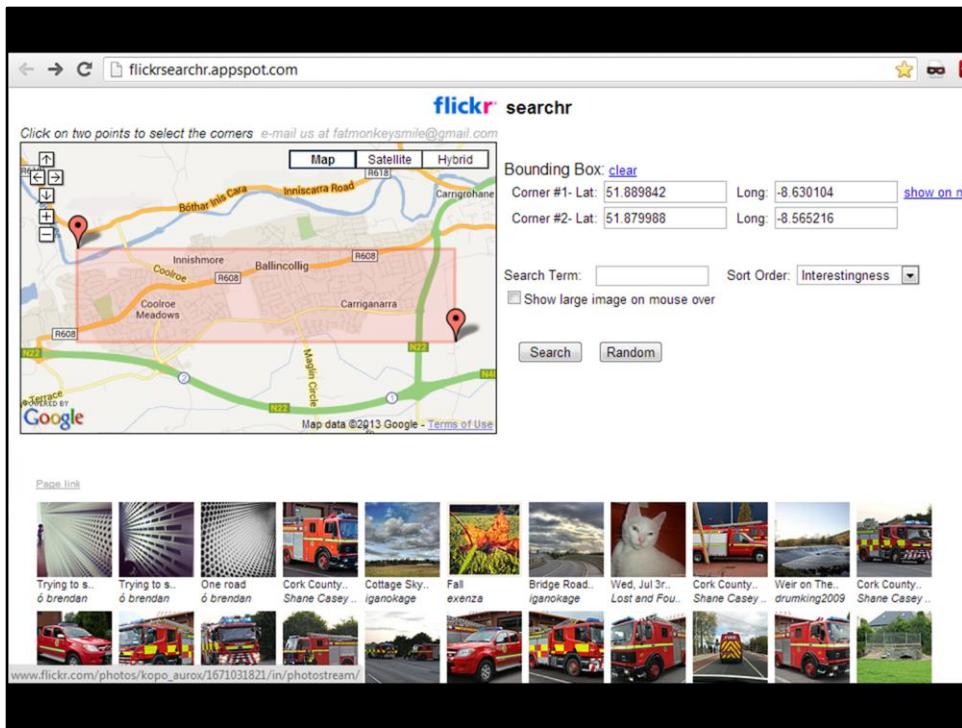
## 4. Pics or it did not happen

---

Cork | Sec

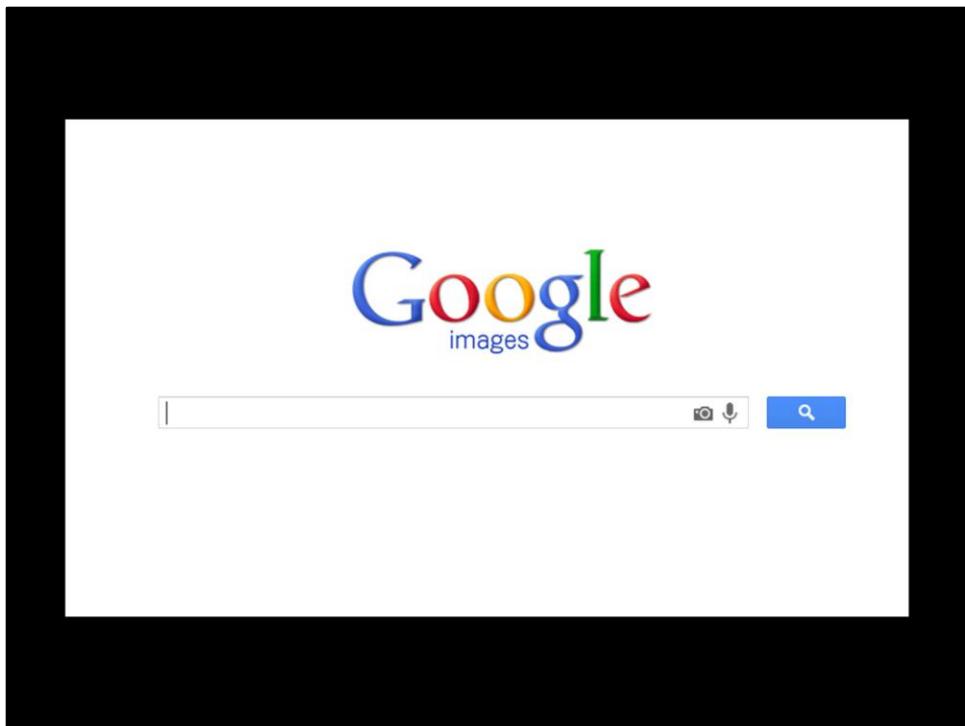
The last category of online tools that are handy for tracking people are related to Pictures. People love to upload pics online – whether that's to Twitter, Flickr, Picasa or Facebook

Pictures are useful when you are tracking someone in a couple of cases. Firstly they can be used to see what sort of pictures have been taken in a certain area, and secondly they can be useful because of the extra hidden data they contain.



FlickrSearcher is a nice site that is really simple and straightforward but which lets you easily get any pictures on flickr that are geotagged and located in an area of your choosing.

## DEMO



If you have an avatar for a person using a reverse image search site can be very helpful to find other places that person may post online. This normally works a lot better if the person is using a picture as opposed to a photo of themselves.

There are two sites in particular to check for this – tineye.com and google image search (which not a lot of people know about)

DEMO – Google – Mikkos Avatar



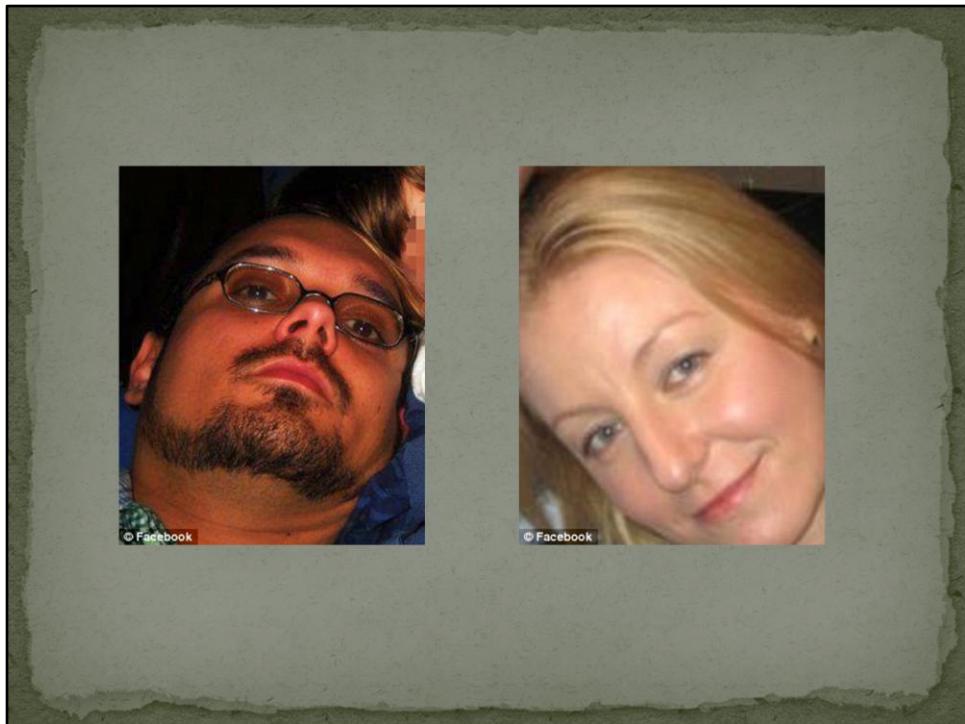
And its also worth mentioning of course EXIF data. I mentioned this earlier on with the maltego mapping of Paris Hilton. Everyone today is walking around with a decent camera in their pocket, and a lot of them will sometimes record interesting EXIF data such as GPS coordinate in the images they upload.

There are several sites that will parse EXIF data but instead of demoing a bunch of them – let me tell you a story about them instead.

This picture was posted on Twitter back in 2012. Apologies to the girls in the room, so heres some simple censorship.

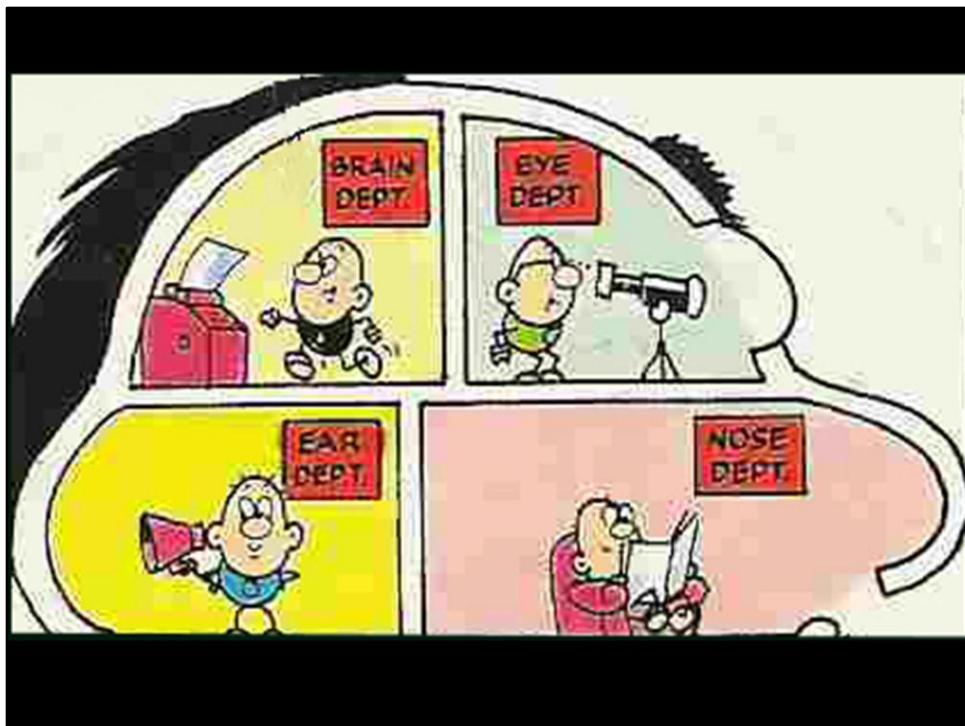
The picture was used on several sites that where defaced by a prolific hacker called WOrmer including at least 4 Law Enforcement sites. What he had not realised was that when using his girlfriends iPhone to take this picture, it also automatically stored the GPS coordinates.

Links: <http://imgops.com/>



Those GPS coordinates led the police straight to the house of a Mr. Higinio Ochoa in Melbourne Australia, where he was living with the person from the photo. Both were arrested.

This is very good case of where a simple mistake can allow someone to go from a piece of information posted online, to knowing where someone lives and ultimately their identity.



So to conclude – we've talked about the sorts of information people put online

We've also looked at some ways that you can track people using People Search sites, Social Networks, Discussion Forums / IRC and also images they post

One final tip that I find invaluable when it comes to tracking people is this "Put yourself in their shoes".

What I've shown so far are a bunch of different tools and portals – and its very tempting to just take any starting data you have and plug it into everything without thinking. Where you will be far more successful though it to start building up a profile of people and try to live their day out in your head. If they have kids – imagine the drive to school, there must be one in a short drives radius – which may help to locate them.

Or look at their twitter posting times – if they post in one big burst in the morning, then lunch and then around 6 – they may have a 9-5 job. Depending on the times they post in the evening you can even figure out if they commute or not

And what if you find out they are single and living in a rural village? Start checking out dating sites...

That ability to put yourself into the mind of another is key for this sort of intelligence work.

- **BE AWARE**
- **AUDIT yourself**
- **Practice good OPSEC**

So lets wrap up with 3 tips on how you stop details about yourself being used to track you!

- Be aware
- Audit yourself
- Good Opsec / Disinformation



Everyone – thanks for coming, and I hope you enjoyed the first part of Cork | Sec (the rest being some beers). Any questions?



So for the rest of the evening – unless anyone else has anything they want to say, feel free to mingle and socialise and grab a beer – or just head on. Try and talk to at least one other person that you had not met before.

In order to be able to run this on a monthly basis we need speakers as well as drinkers – so if you have any topic that you are interested in chatting about, please don't be afraid – and do let me know in the next two weeks. The talks do not need to be polished at all – this is a great setting to try out some ideas you are working on . And even if you don't have a full 40 mins – no issue either we can put a few talks together.

Oh and don't forget to check out CorkSec.RobertMcArdle.com