

Open Source Information Gathering

Chris Gates
carnal0wnage

Shameless Self Promotion

- Blogger...carnal0wnage.attackresearch.com.
- Metasploit Project.
- Attack Research.
- Security Twit → carnal0wnage.
- Want more? Use what I'm about to teach you...or just ask...I like hoegaarden.

Hoegaarden

Information Gathering

Denotes the collection of information before the attack.

The idea is to collect as much information as possible about the target which may be valuable later.

-Christian Martorella

Edge-Security

Fist Conference 2009

<http://www.fistconference.org/>

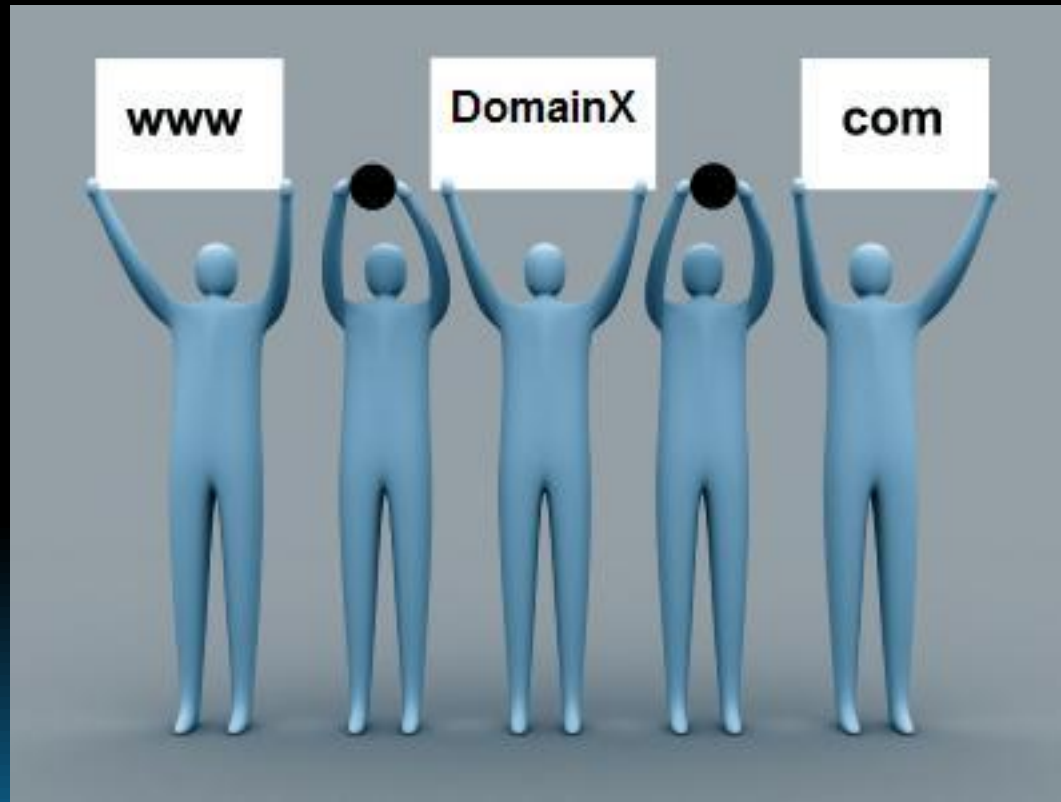
OSINT

Open Source **INT**elligence

“Is an information processing discipline that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.”

http://en.wikipedia.org/wiki/Open_Source_Intelligence

We want to turn...



Into...

```
File Edit View Terminal Tabs Help
msf exploit(ms06_067_keyframe) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\User\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 172.16.2.9
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.1

C:\Documents and Settings\User\Desktop>
```

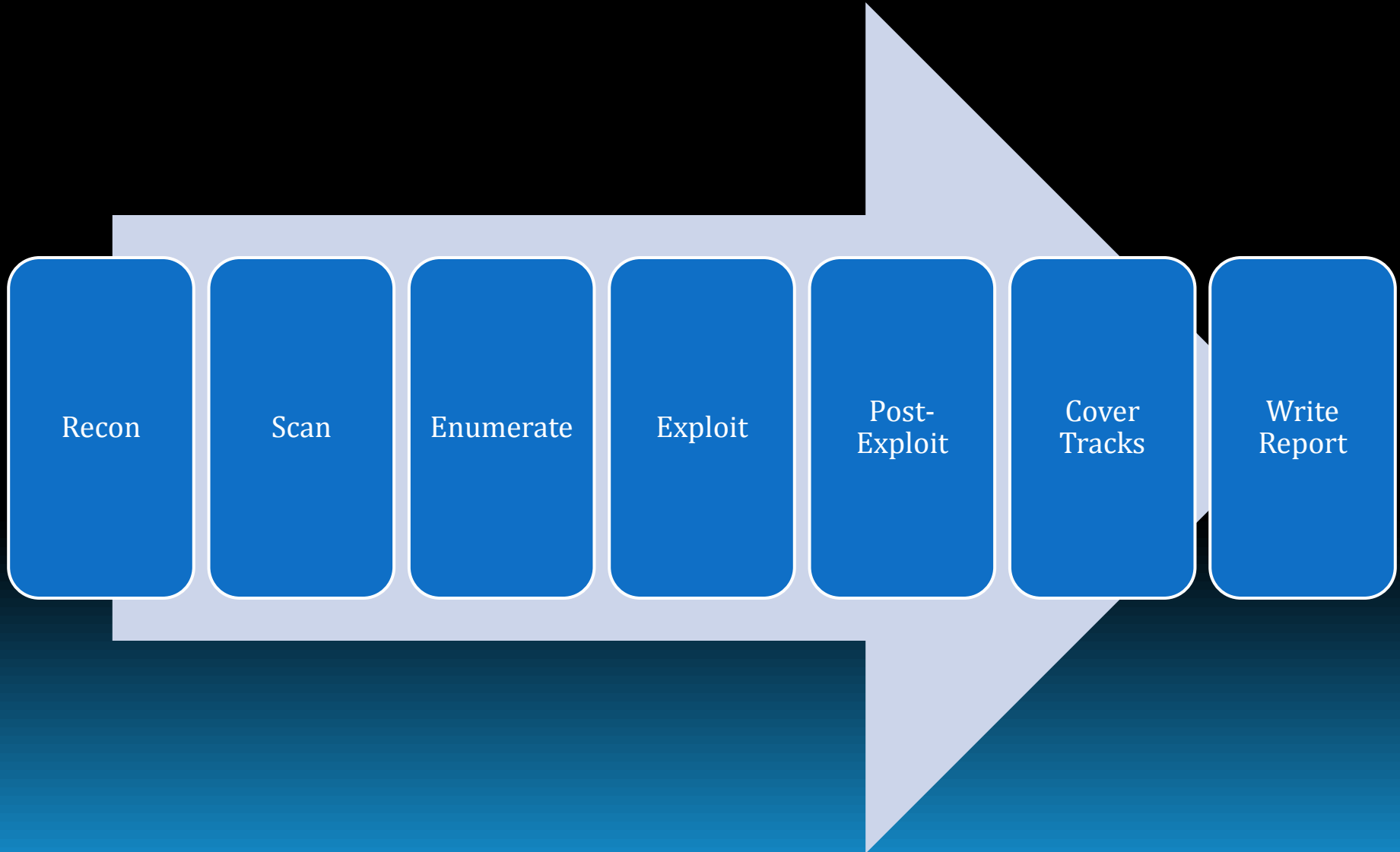
Or...



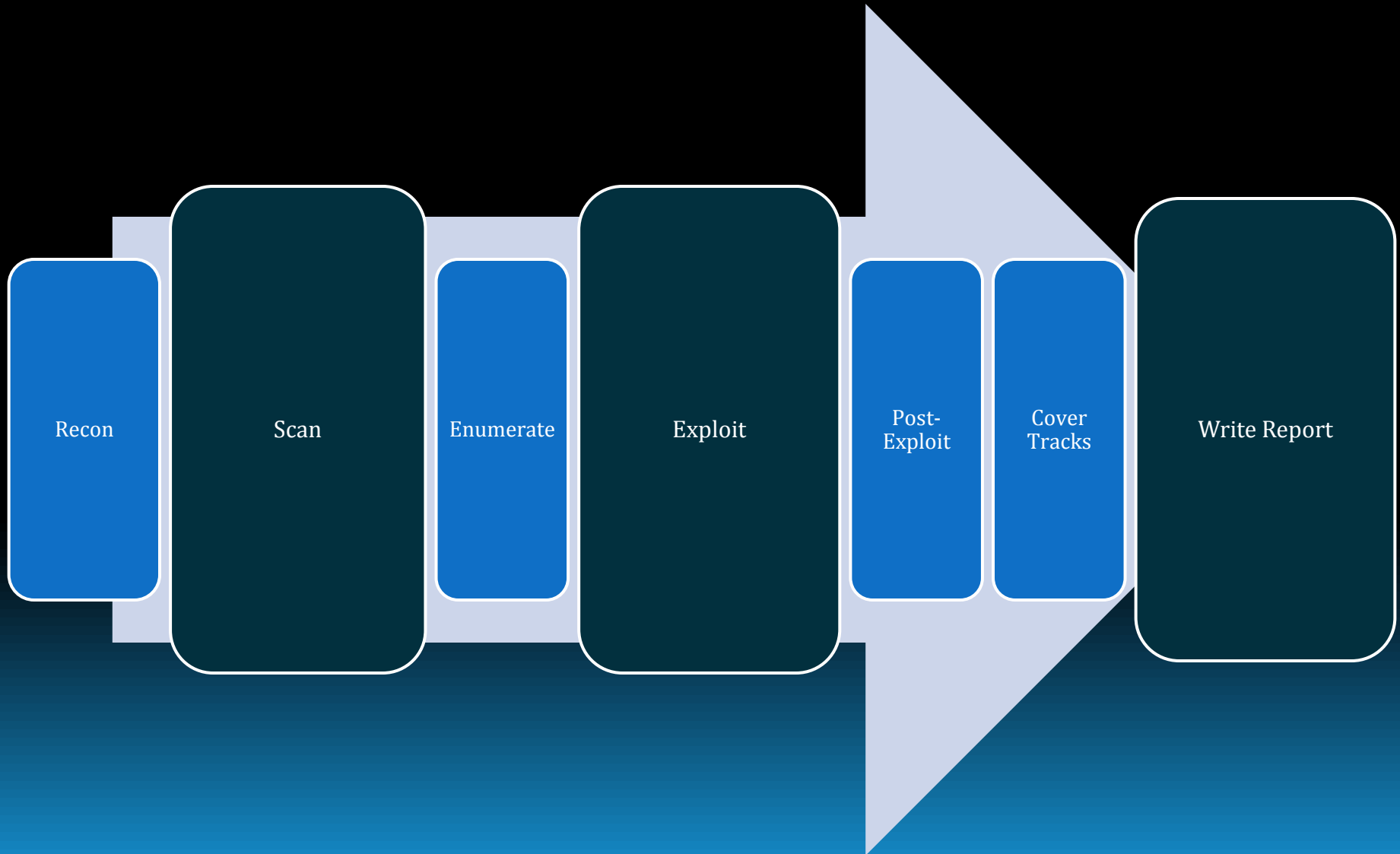
Why Do OSINT?

- Open Source Intelligence Gathering is your critical first step to Full Scope Pentesting or Real World attacking.
 - It simulates REAL WORLD reconnaissance.
 - Anything on the net is in scope.... Users are fair game for client-sides.
 - Any boxes you own are in scope.... No boxes are off limits.
 - Do you know what information you, your employees, or your company has put out there?

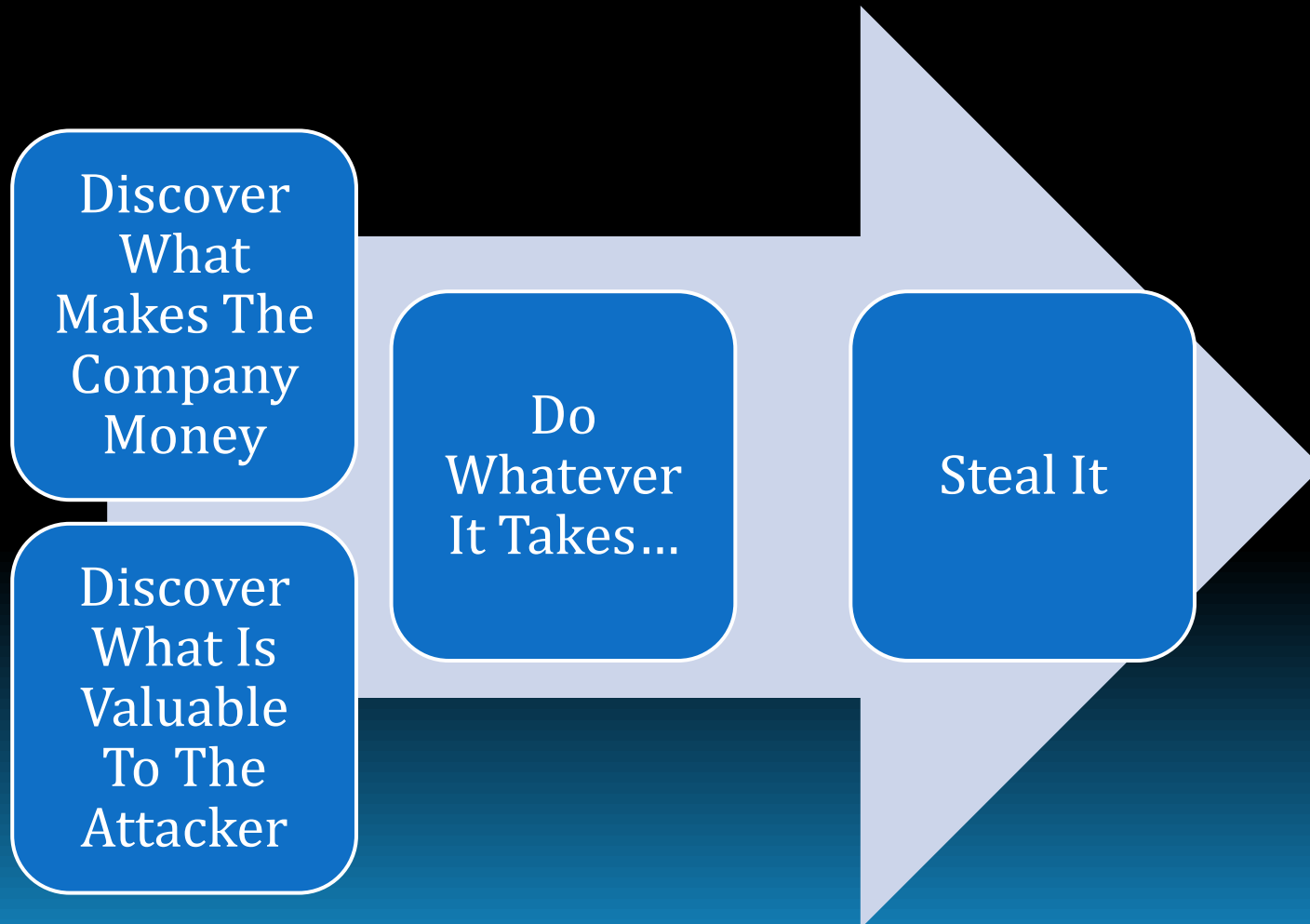
Typical Pentesting Methodology



What We Focus On Currently



Real World Hacking Methodology



Definitions!?

- A few definitions to get out of the way...I'll try to make it as painless as possible.
- But, we're going have to **read**...yeah sad face.



Types of Information Gathering

- Passive
- Semi-Passive
- Active

- Category Descriptions

From <http://www.paterva.com/web3/services/information-gathering-service/>

Passive Information Gathering

- Passive
 - Great care is taken to ensure that the target organization does not detect the profiling. This means that no packets can ever be sent to the target.
 - This type of profiling is typically **time intensive**.

NO TRAFFIC

- From <http://www.paterva.com/web3/services/information-gathering-service/>

Semi-Passive Information Gathering

- Semi-Passive
 - Profiling the target with methods that would appear to the target as normal Internet traffic and behavior.

NORMAL TRAFFIC

- From <http://www.paterva.com/web3/services/information-gathering-service/>

Active Information Gathering

- Active
 - This type of profiling **should** be detected by the target organization.
 - Actively seeking out new/unpublished servers, directories, files, documents along with full network visibility scans.

ABNORMAL TRAFFIC

- From <http://www.paterva.com/web3/services/information-gathering-service/>

Categories of Information Gathering

- Two General Types
 - Infrastructure.
 - People / Organization.

Infrastructure Information Gathering

- Infrastructure
 - Every organization with an Internet presence requires some form of infrastructure to support that presence. That information is what we want to discover.
 - Infrastructure profiling is far easier to do and **automate** than people/organization profiling which is more manual.

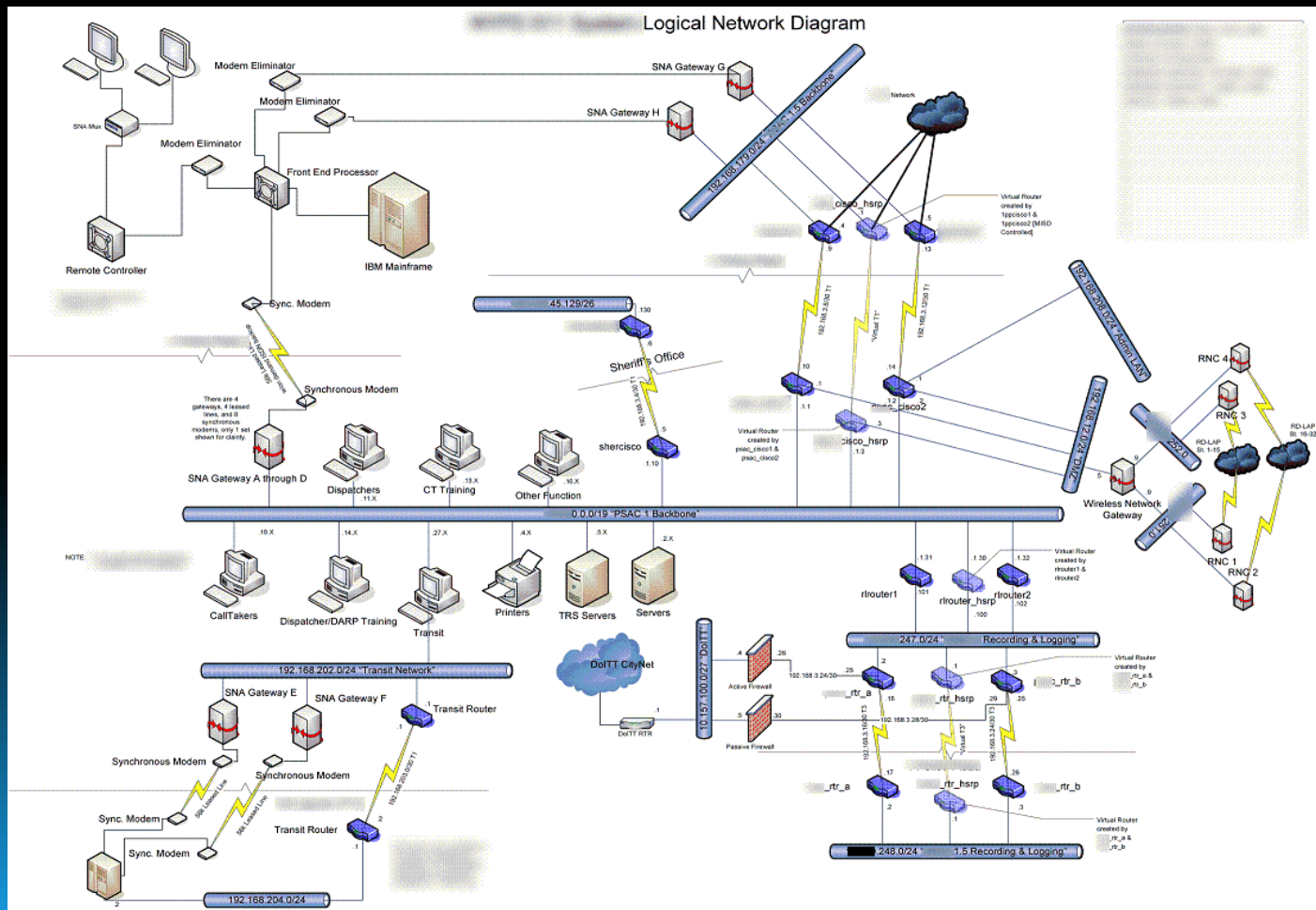
Categories of Information Gathering

- Infrastructure



Categories of Information Gathering

- Infrastructure



People/Organization Information Gathering

- People / Organization
 - Every organization requires people to support that organization. How runs the company? Who runs IT? Who runs finance/HR? That information is what we want to discover.
 - People / Organization profiling is much more difficult to do and **automate** than infrastructure. Which John Doe is the right one?

Categories of Information Gathering

- People / Organization



Where Does This Information Come From?

- Web 2.0...How I <3 thee...
- Public data and records.
- Information that is mandatory for the Internet (DNS, whois, MX).
- Private data we pay for i.e. Lexis Nexis/Choice Point/Find a Friend/Spoke/Zoominfo.
- Data placed there by the target.
- Data placed there by the target's users.



How Do We Find It?

- Information that is mandatory for the Internet.
 - DNS, MX, Web.
 - Whois.
- Data placed there by the target.
 - Voluntarily.
 - Required by State/Federal law.
- Data placed there by the target's users.
 - Voluntarily.
 - Required by State/Federal law.

Considerations

- Tons of Information.
 - Can be hard to sort through.
 - Some data gathering/analysis can be automated.
 - Maltego!
 - And other tools.
 - Other data needs a human to sort through.
 - Brain!
 - But now Maltego Mesh can help



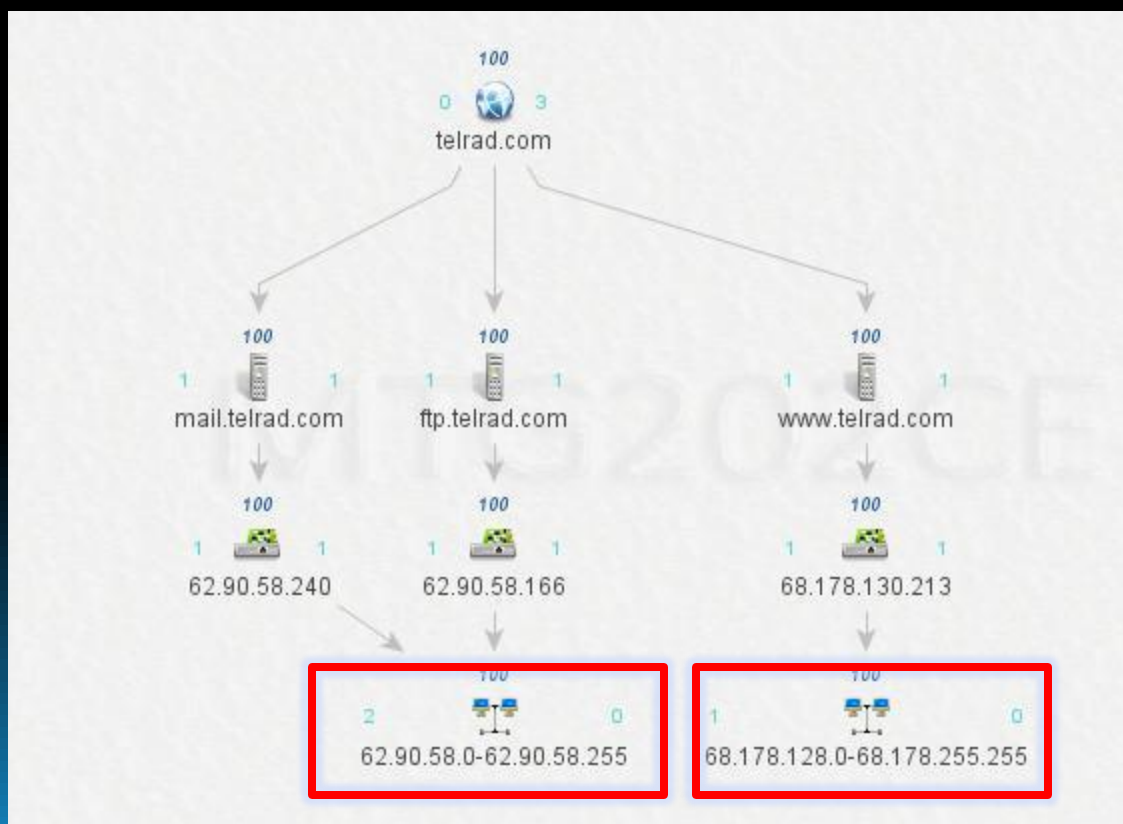
Practical Examples

Infrastructure Intelligence Gathering

- How would you like to discover ALL networks/netblocks a target organization owns.
- How would you like to discover a target organization's presence in other countries (.co.uk, .de, .be, etc).
- We want to build that infrastructure diagram without the target knowing we are doing it!

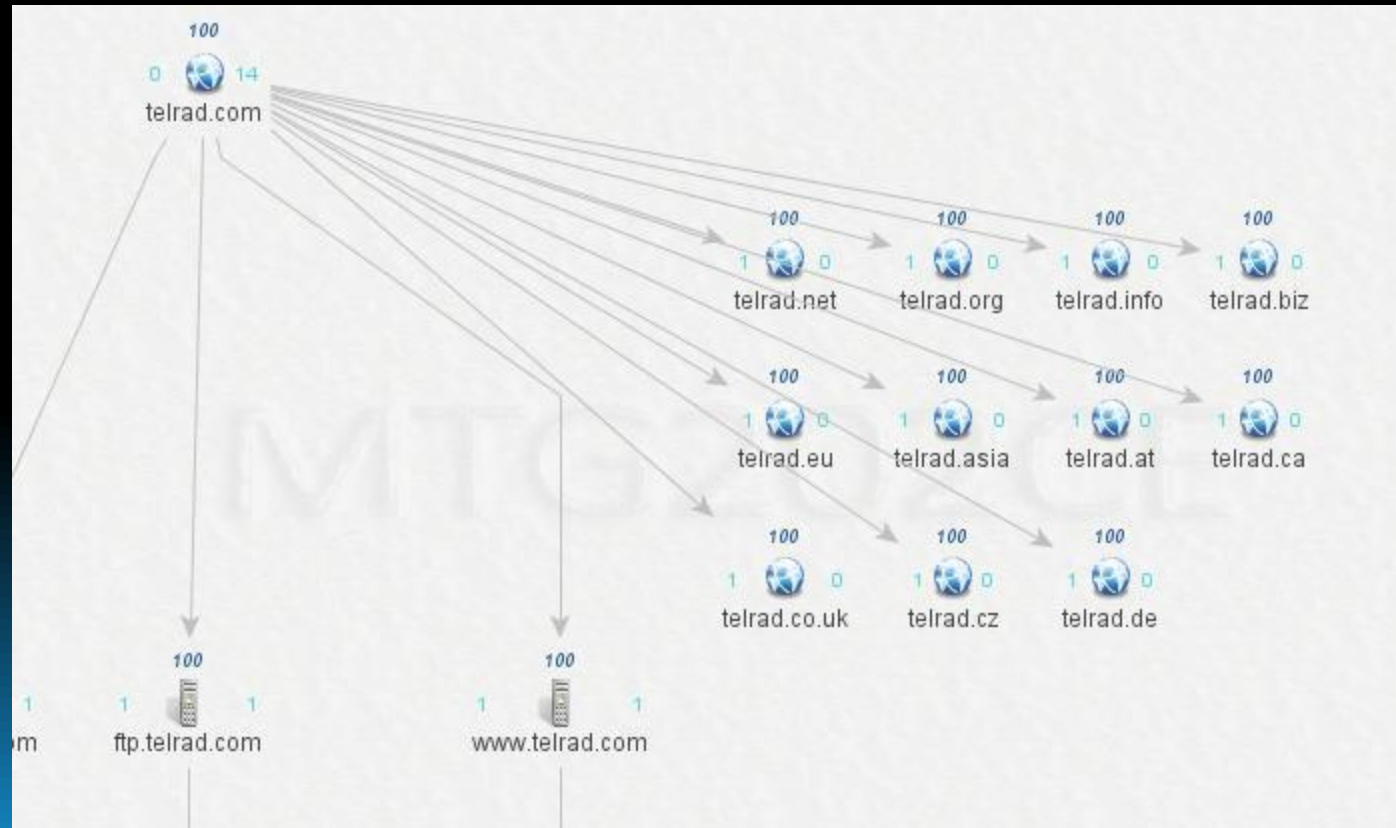
Infrastructure: Identify Other Netblocks

- Identify other networks/netblocks



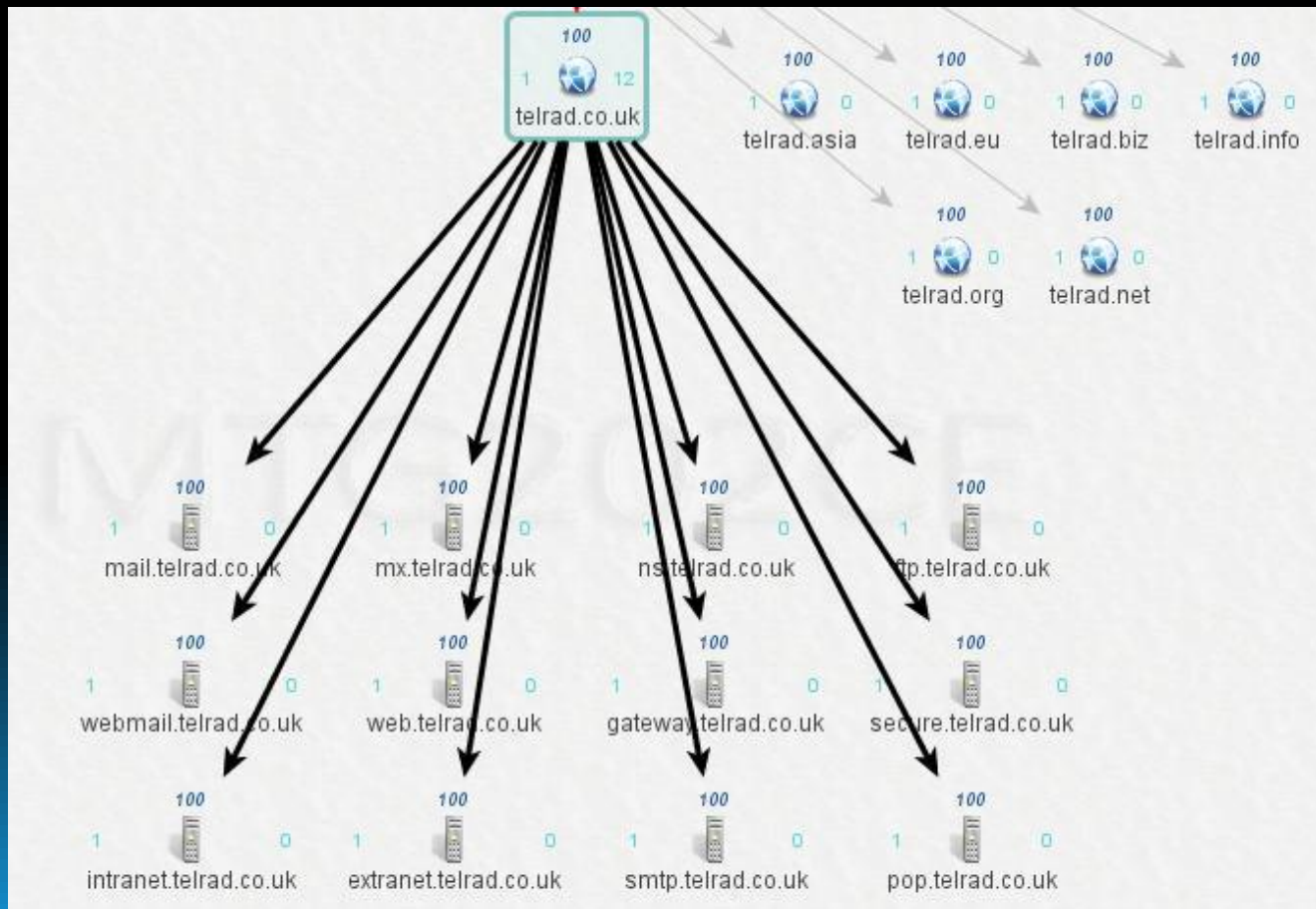
Infrastructure: Discover Other TLDs

- Expand out to other TLDs



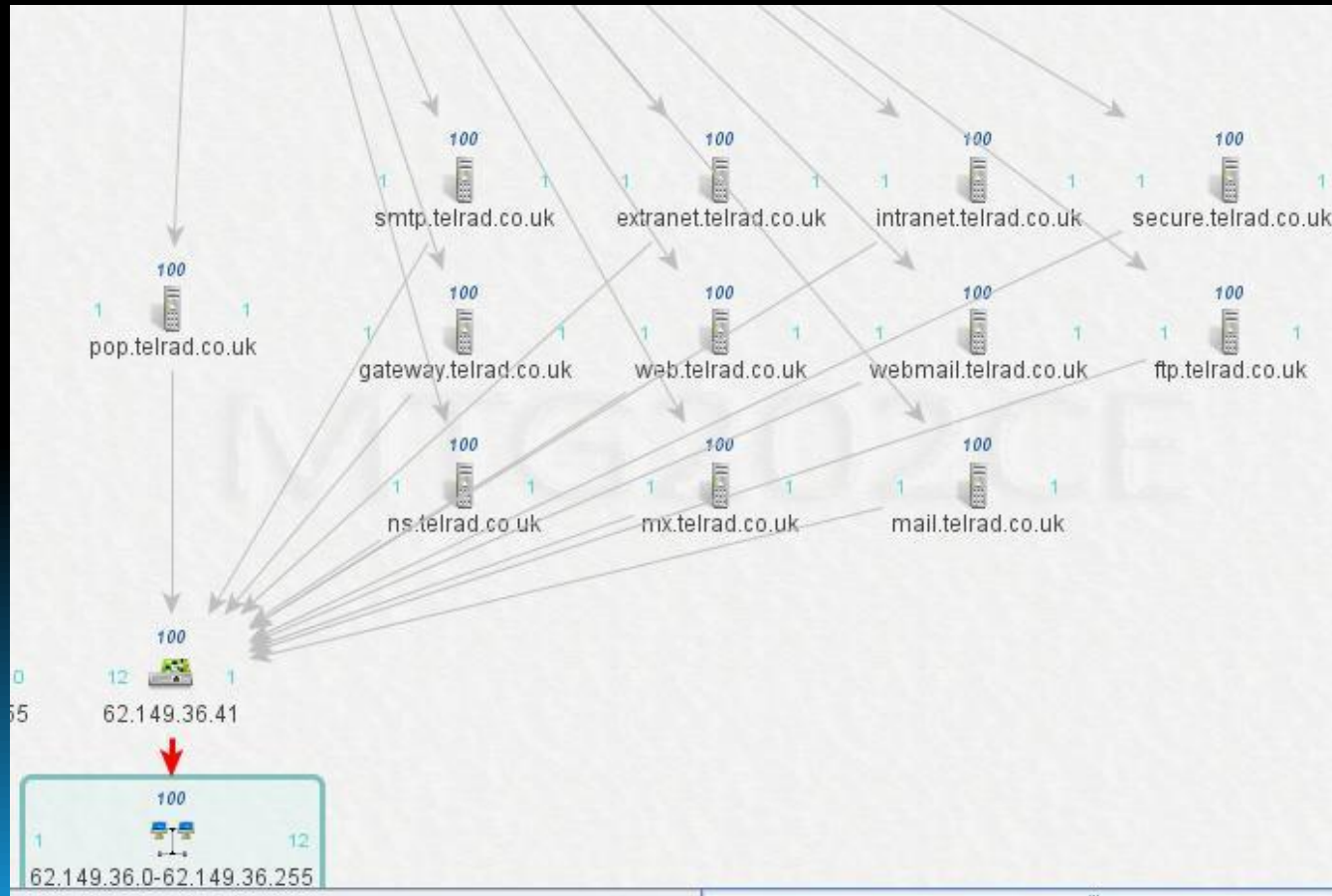
Infrastructure: Bruteforce DNS names

- Bruteforce DNS names

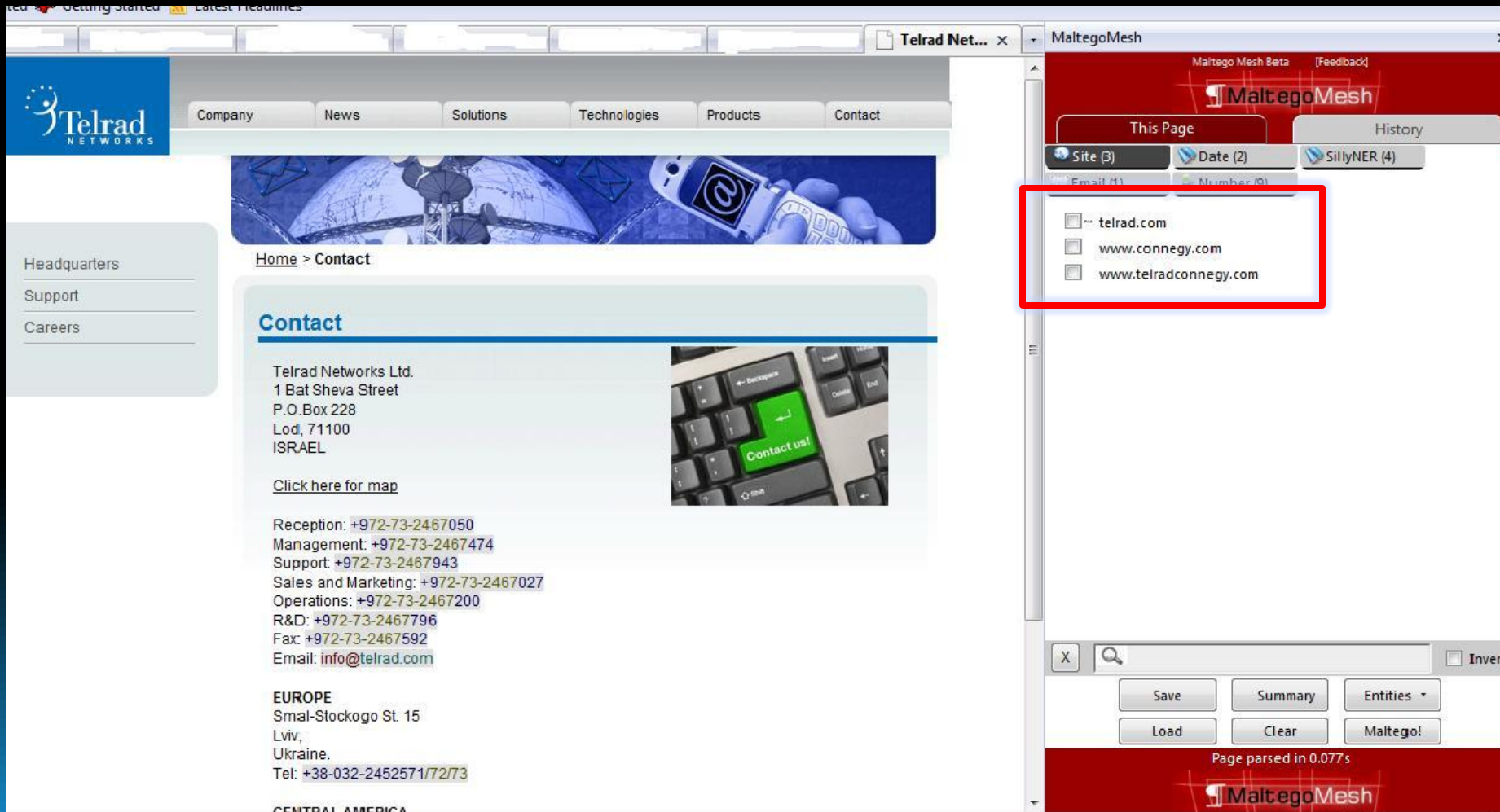


Infrastructure: Identify Even More Netblocks

- Find more net blocks



Infrastructure: Using Maltego Mesh



The screenshot shows a web browser with two tabs: 'Telrad Net...' and 'MaltegoMesh'. The Telrad Networks website is visible in the background, featuring a navigation menu with 'Company', 'News', 'Solutions', 'Technologies', 'Products', and 'Contact'. The 'Contact' page is active, displaying contact information for Telrad Networks Ltd. in Israel and Europe. The Maltego Mesh interface is overlaid on the right side of the browser window. It has a red header with 'Maltego Mesh Beta' and '[Feedback]'. Below the header, there are tabs for 'This Page' and 'History'. Under 'This Page', there are filters for 'Site (3)', 'Date (2)', and 'SillyNER (4)'. A list of entities is displayed, with a red box highlighting the following items:

- telrad.com
- www.connegy.com
- www.telradconnegy.com

At the bottom of the Maltego Mesh interface, there are buttons for 'Save', 'Summary', 'Entities', 'Load', 'Clear', and 'Maltego!'. The status bar at the bottom indicates 'Page parsed in 0.077s'.

Infrastructure: Useful Tools

- Tools to get it done
 - Maltego
 - ServerSniff.net
 - Robtex.com
 - Clez.net
 - CentralOps.net
 - Rsnake's fierce.pl
 - PassiveRecon Firefox Plugin



People/Organization Intelligence Gathering

- To create personnel & organization profiles, deliver client-side attacks, or prepare for Social Engineering engagements we gather information on a organization's users or a particular user.
- What information has been placed in the public domain by the company or its users?
- Can I identify key personnel? Can I develop an understanding of corporate culture?

People / Organization: Email Harvesting

- Harvest Email Addresses



```
user@titanium:~/pentest/InfoGather/theHarvesterV1.4$ python theHarvester.py -d telrad.com -l 5000 -b linkedin
```

```
*****
*TheHarvester Ver. 1.4b          *
*Coded by Christian Martorella   *
*Edge-Security Research         *
*cmartorella@edge-security.com   *
*****

Searching for telrad.com in linkedin :
=====

Total results: 376
Limit: 376
Searching results: 0
Searching results: 100
Searching results: 200
Searching results: 300
```

```
Accounts found:
=====

Dror Pockard
Rahme Mehmet
Dani Zilberstein
Oksana Nahibina
Itshak Aizner
Uriel Hassidim
Walt Nestell
Opher Yaron
Oleg Zaslavski
Debi Zylbermann
Irina Rossovsky
Avinoam Kialy
Nazar Chorny
```

```
user@titanium:~/pentest/InfoGather/theHarvesterV1.4$ python theHarvester.py -d telrad.com -l 5000 -b pgg
```

```
*****
*TheHarvester Ver. 1.4b          *
*Coded by Christian Martorella   *
*Edge-Security Research         *
*cmartorella@edge-security.com   *
*****
```

```
Searching for telrad.com in pgg :
=====
```

```
oleksiyz@telrad.com
Searching for connegy.com in google :
=====

Total results: 6150
Limit: 500
Searching results: 0
Searching results: 100
Searching results: 200
Searching results: 300
Searching results: 400
```

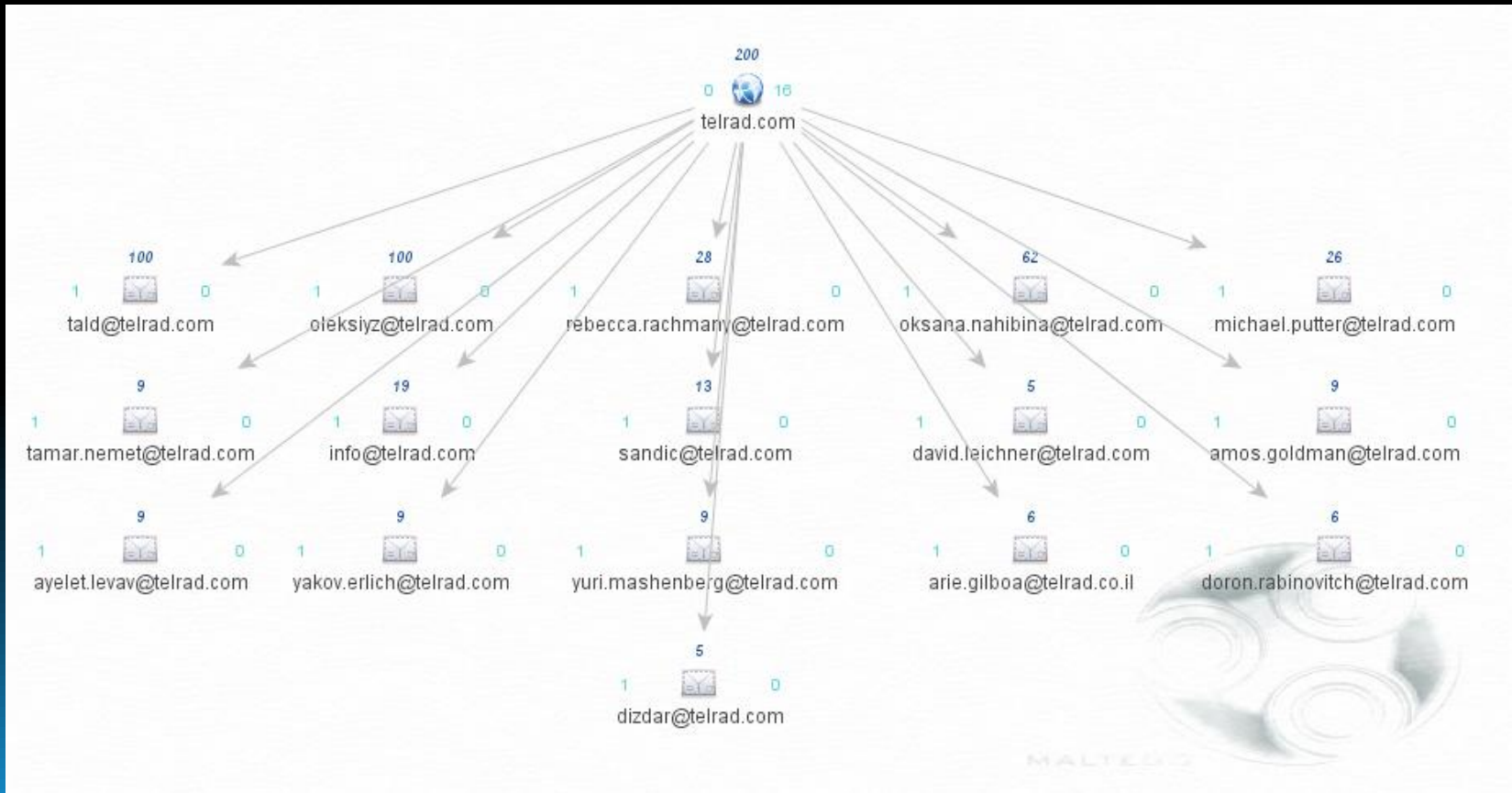
```
Accounts found:
=====

jobs@connegy.com
ortal@connegy.com
info@connegy.com
shlomo.haik@connegy.com
=====
```

```
Total results: 4
```

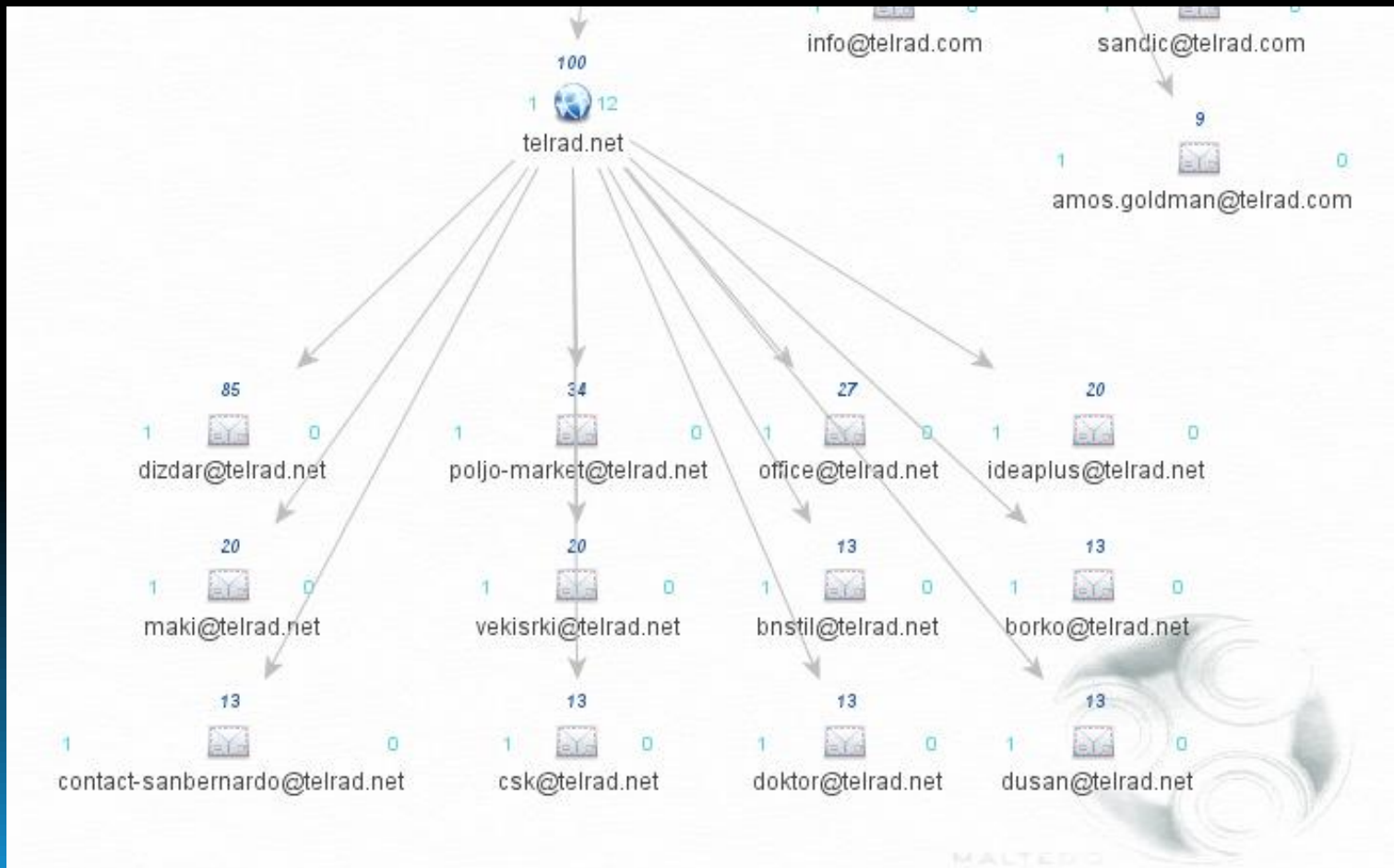
People / Organization: Email Harvesting

- Harvest Email Addresses



People / Organization: Email Harvesting

- Harvest Email Addresses
 - Searching for other TLDs was handy.

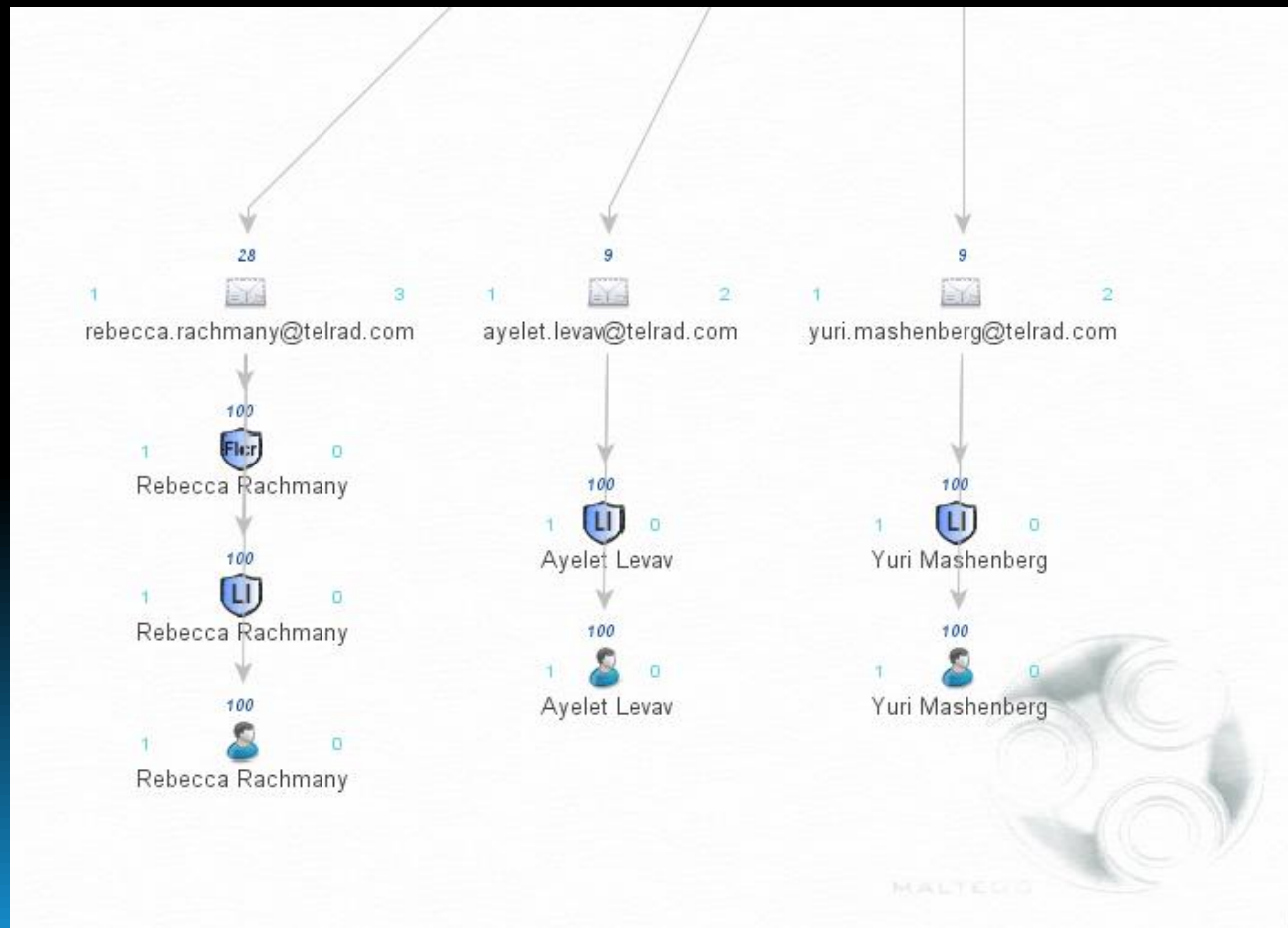


People / Organization: Email Harvesting

MALTEGO²



- Emails can be turned into users.



People / Organization: Email Harvesting

- Which can be turned into new friends and associates.

```
user@titanium:~/pentest/InfoGather/theHarvester
-l 5000 -b linkedin
```

```
*****
*TheHarvester Ver. 1.4b          *
*Coded by Christian Martorella  *
*Edge-Security Research        *
*cmartorella@edge-security.com  *
*****
```

```
Searching for telrad.com in linkedin :
=====
```

```
Total results: 376
Limit: 376
Searching results: 0
Searching results: 100
Searching results: 200
Searching results: 300
```

```
Accounts found:
=====
```

```
Dror Pockard
Rahme Mehmet
Dani Zilberstein
Oksana Nahibina
Itshak Aizner
Uriel Hassidim
Walt Nestell
Opher Yaron
Oleg Zaslavski
Debi Zylbermann
Irina Rossovsky
Avinoam Kialy
Nazar Chorny
```


« Go back to Search Results | « Prev
People

Ayelet Levav



VP Human Resources at Telrad Networks Ltd.

Israel | Telecommunications

Current

- VP Human Resources at Telrad Networks Ltd. 

Past

- director of Human Resources at Amdocs 
- Human Resources Manager at Geo Interactive Media Group (Emblaze)
- Assistant to VP HR at vcon 

Education

- Tel Aviv University
- Hadasim
- Hadassim

Connections

27 connections

Public Profile

<http://www.linkedin.com/pub/ayelet-levav/1/960/449>

➔ **Send InMail**

➔ **Add Ayelet to your network**

➔ **Forward this profile to a connection**

Ads by LinkedIn Members

DCconfidential.com

The elite discreet job placement firm for DC area IT Professionals!

[DCconfidential.com](#)

From: Hippopotamus Productions Inc.

HELP NET SECURITY

Help Net Security

Daily Computer and Network Security News and Articles.


www.net-security.org

From: Berislav Kucan [What's this?](#)

Ayelet Recommends (1)

Merav Yanai, *Executive recruiting manager, Nisha*

« Excellent business and people understanding,...

 Expanded profile views are available only to premium account holders. [Upgrade your account.](#)

Contact Settings

Interested In

- job inquiries
- expertise requests
- business deals
- reference requests
- getting back in touch

People / Organization: Email Harvesting Tools

- Tools to get it done

- Maltego



- theHarvester



- PassiveRecon Firefox Plugin



People / Organization: Document Metadata

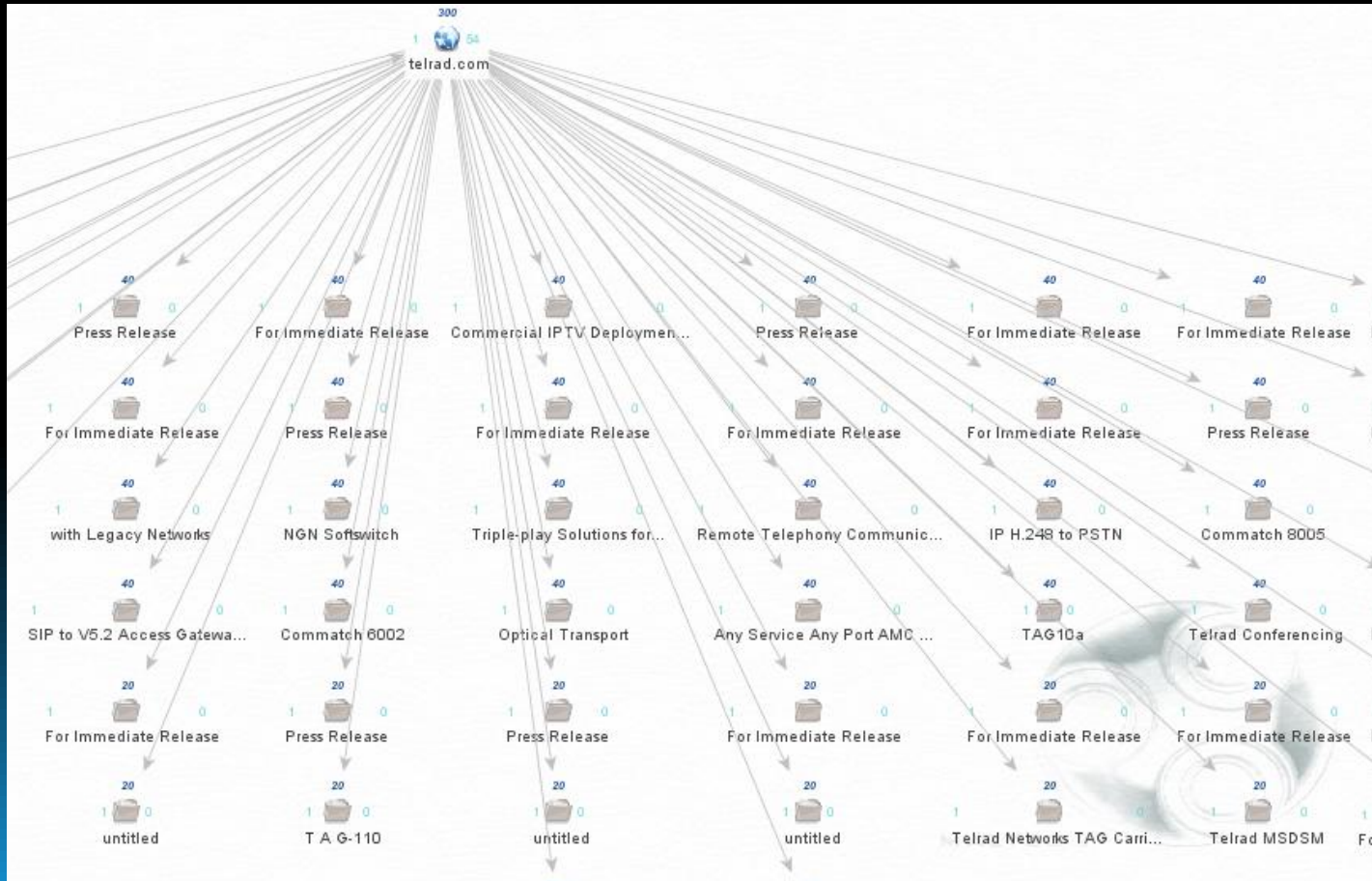
- Documents contain all sort of useful information
 - Useful Extensions.

.pst	.cfg	.pcf	.pdf	.qmd	.tax	.dif
.doc	.docx	.xls	.xlsx	.ppt	.pptx	.dbf
.qdb	.qsd	.qtx	.idx	.qif	.mny	.txt
.odt	.ods	.odp	.ofx	.ofc	.vcf	.rtf

- ****Not a full list****

People / Organization: Document Metadata

- Documents contain all sort of useful information



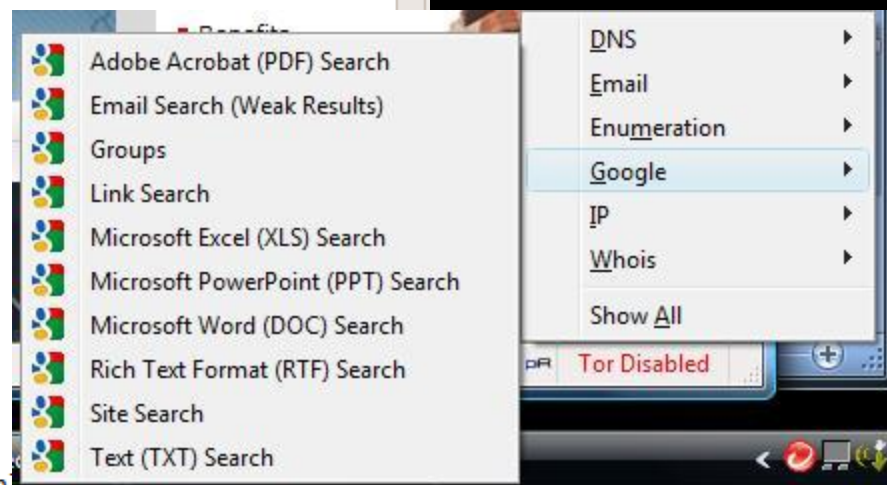
People / Organization: Document Metadata

- Documents contain all sort of useful information

```
user@titanium:~/pentest/InfoGather/metagoofil-1.4a$ python metagoofil.py -d telrad.com -l 500 -f all -o telrad-all.html -t telrad-all.com

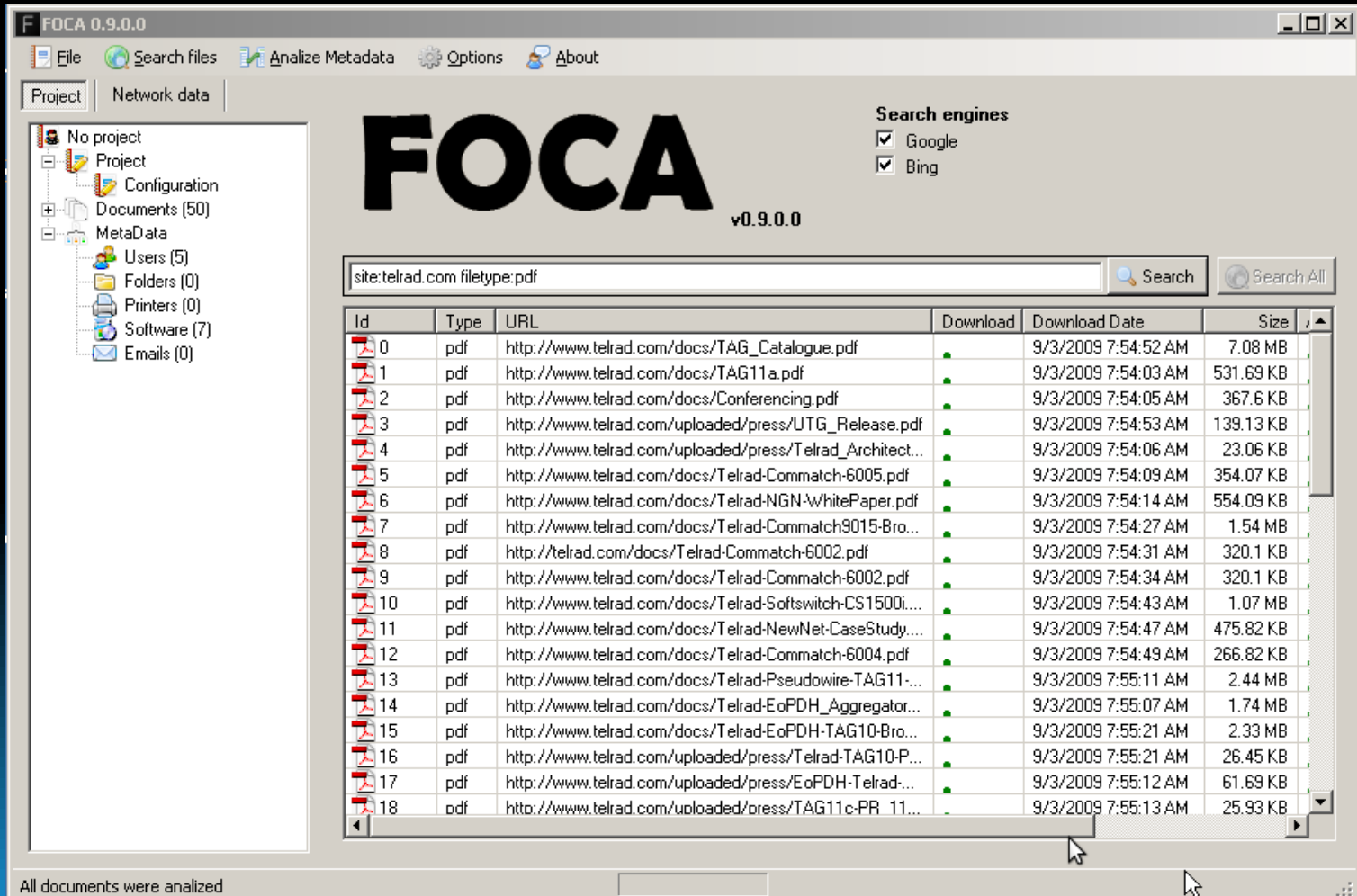
*****
*MetaGooFil Ver. 1.4a          *
*Coded by Christian Martorella *
*Edge-Security Research       *
*cmartorella@edge-security.com *
*****

[+] Command extract found, proceeding with leeching
[+] Searching in telrad.com for: pdf
[+] Total results in google: 48
[+] Limit: 48
[+] Searching results: 0
[+] Searching results: 20
[+] Searching results: 40
[ 1/51 ] https://www.google.com/accounts/Login?hl=en&continue=http://www.google.com/search%3Fnum%3D20%26start%3D0%26hl%3Den%26btnG%3DB%25C3%25BA%26q%3Dsite:telrad.com%2Bfiletype:pdf
```



People / Organization: Document Metadata

- FOCA



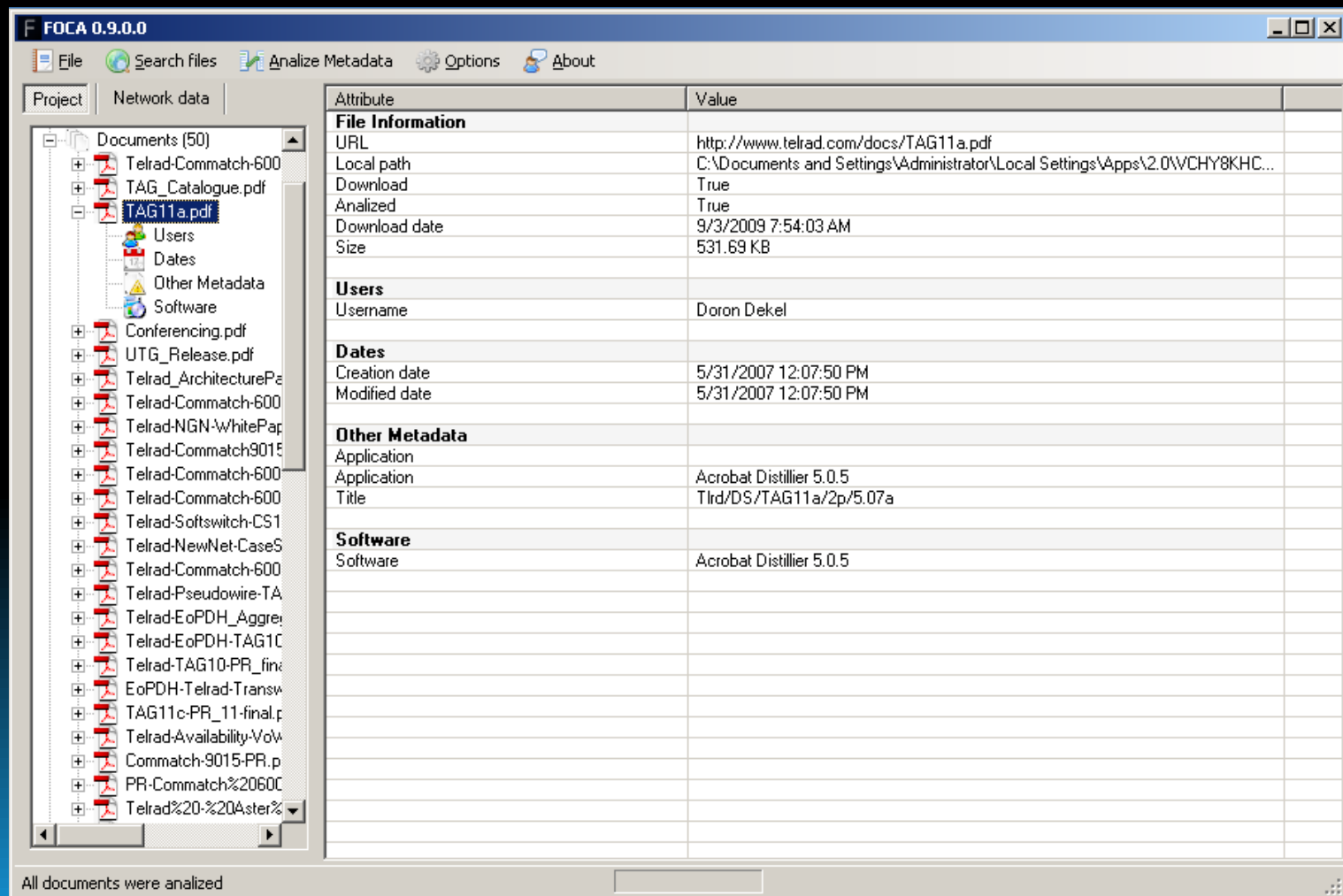
The screenshot shows the FOCA 0.9.0.0 application window. The interface includes a menu bar (File, Search files, Analyze Metadata, Options, About), a toolbar, and a sidebar with a project tree. The main area displays the FOCA logo and version number (v0.9.0.0). A search bar contains the query "site:telrad.com filetype:pdf". Below the search bar is a table of search results.

Id	Type	URL	Download	Download Date	Size
0	pdf	http://www.telrad.com/docs/TAG_Catalogue.pdf	●	9/3/2009 7:54:52 AM	7.08 MB
1	pdf	http://www.telrad.com/docs/TAG11a.pdf	●	9/3/2009 7:54:03 AM	531.69 KB
2	pdf	http://www.telrad.com/docs/Conferencing.pdf	●	9/3/2009 7:54:05 AM	367.6 KB
3	pdf	http://www.telrad.com/uploaded/press/UTG_Release.pdf	●	9/3/2009 7:54:53 AM	139.13 KB
4	pdf	http://www.telrad.com/uploaded/press/Telrad_Architect...	●	9/3/2009 7:54:06 AM	23.06 KB
5	pdf	http://www.telrad.com/docs/Telrad-Commatch-6005.pdf	●	9/3/2009 7:54:09 AM	354.07 KB
6	pdf	http://www.telrad.com/docs/Telrad-NGN-WhitePaper.pdf	●	9/3/2009 7:54:14 AM	554.09 KB
7	pdf	http://www.telrad.com/docs/Telrad-Commatch9015-Bro...	●	9/3/2009 7:54:27 AM	1.54 MB
8	pdf	http://telrad.com/docs/Telrad-Commatch-6002.pdf	●	9/3/2009 7:54:31 AM	320.1 KB
9	pdf	http://www.telrad.com/docs/Telrad-Commatch-6002.pdf	●	9/3/2009 7:54:34 AM	320.1 KB
10	pdf	http://www.telrad.com/docs/Telrad-Softswitch-CS1500i...	●	9/3/2009 7:54:43 AM	1.07 MB
11	pdf	http://www.telrad.com/docs/Telrad-NewNet-CaseStudy...	●	9/3/2009 7:54:47 AM	475.82 KB
12	pdf	http://www.telrad.com/docs/Telrad-Commatch-6004.pdf	●	9/3/2009 7:54:49 AM	266.82 KB
13	pdf	http://www.telrad.com/docs/Telrad-Pseudowire-TAG11...	●	9/3/2009 7:55:11 AM	2.44 MB
14	pdf	http://www.telrad.com/docs/Telrad-EoPDH_Aggregator...	●	9/3/2009 7:55:07 AM	1.74 MB
15	pdf	http://www.telrad.com/docs/Telrad-EoPDH-TAG10-Bro...	●	9/3/2009 7:55:21 AM	2.33 MB
16	pdf	http://www.telrad.com/uploaded/press/Telrad-TAG10-P...	●	9/3/2009 7:55:21 AM	26.45 KB
17	pdf	http://www.telrad.com/uploaded/press/EoPDH-Telrad...	●	9/3/2009 7:55:12 AM	61.69 KB
18	pdf	http://www.telrad.com/uploaded/press/TAG11c-PR_11...	●	9/3/2009 7:55:13 AM	25.93 KB

At the bottom of the window, a status bar indicates "All documents were analyzed".

People / Organization: Document Metadata

- FOCA



The screenshot shows the FOCA 0.9.0.0 application window. The left pane displays a file tree with 'TAG11a.pdf' selected. The right pane shows a table of metadata attributes and values for this document.

Attribute	Value
File Information	
URL	http://www.telrad.com/docs/TAG11a.pdf
Local path	C:\Documents and Settings\Administrator\Local Settings\Apps\2.0\WCHY8KHC...
Download	True
Analyzed	True
Download date	9/3/2009 7:54:03 AM
Size	531.69 KB
Users	
Username	Doron Dekel
Dates	
Creation date	5/31/2007 12:07:50 PM
Modified date	5/31/2007 12:07:50 PM
Other Metadata	
Application	
Application	Acrobat Distillier 5.0.5
Title	Tlrd/DS/TAG11a/2p/5.07a
Software	
Software	Acrobat Distillier 5.0.5

All documents were analyzed

People / Organization: Document Metadata

Metagoofil

- Metadata to discover usernames

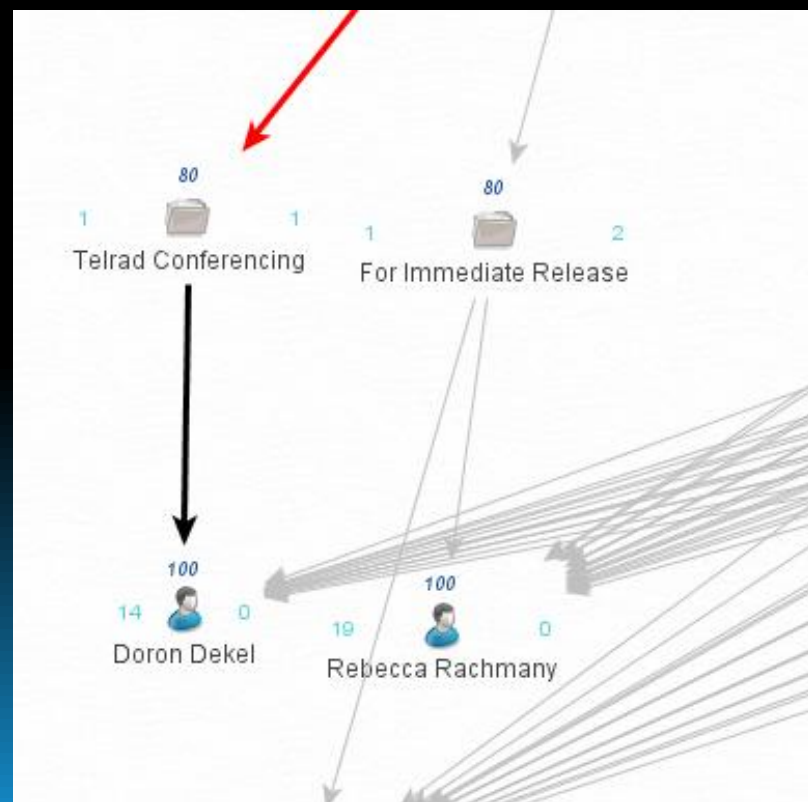
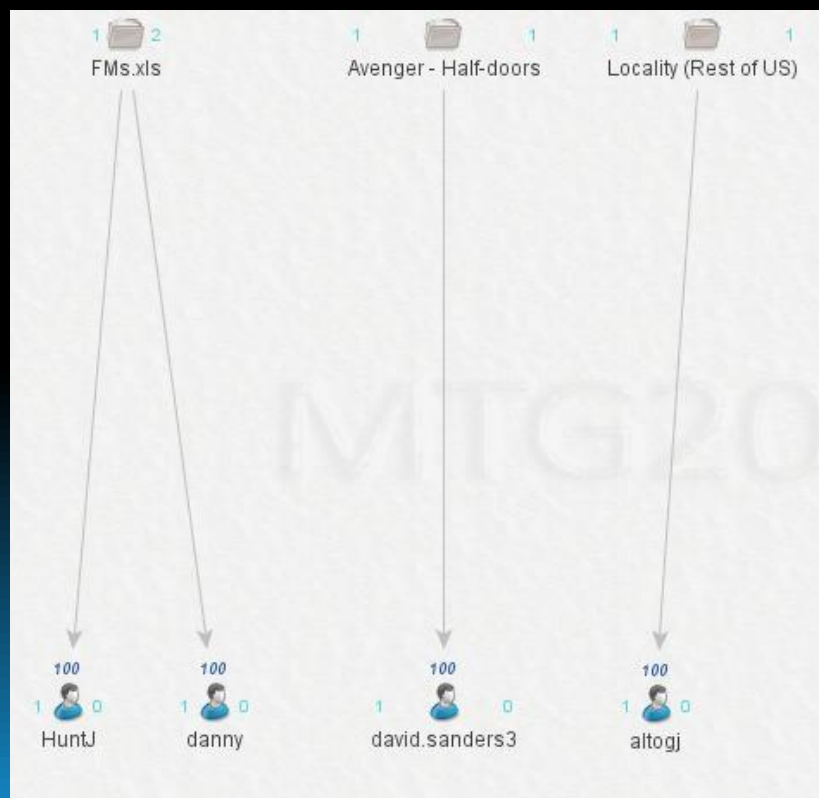
Total authors found (potential users):

```
taylorm
kim.conner
M. Faye Messick
lsebring
tirochk
greta.alto
TrecekRR
DOD User
bchapman
beth.kay.chapman
ls
Suk Miller
altog
CEJKAC
SUTMAN NANCY
Darryll G. Smith
INBURFOR
kenneth bodenheimer
Laurie Bodenheimer
jbarbie
lbishop
AHARRIS
JacksonR
Bobbie Jackson
OlsonC
Clancy Olson Jr.
trt
KakelA
charles.blumenfeld
GRP7-FRC
MWR
powellg
Powell, Gayle
8bde.local
david.sanders3
Lynn Akbar
ACS, Relocation
.
```

```
mmessick
hfowler
Tracy L. Neth
swinglel
765thCMDS
Todd Barrett
me
OSJA
Collena Rodriguez
user
Unknown
BDM_PC
altogj
Laura Lawrence
Administrator
kleader
OPM
LJLAWREN
James M. Farron
TPEHRENZ
Parsonsc
TRWUser
Russ Dulaney
James/Mariela
Jason.Hudson
robin.carper
Patricia Reyes
Defense Security Service
kate.lugo
RodleyD
Myers
DennoA
Donald.McWhorter
james.collazo
tempclass
Sue Jarrett
```

People / Organization: Document Metadata

- Metadata to discover usernames
 - ▣ Use Maltego to link usernames to people on the web.



People / Organization: Document Metadata

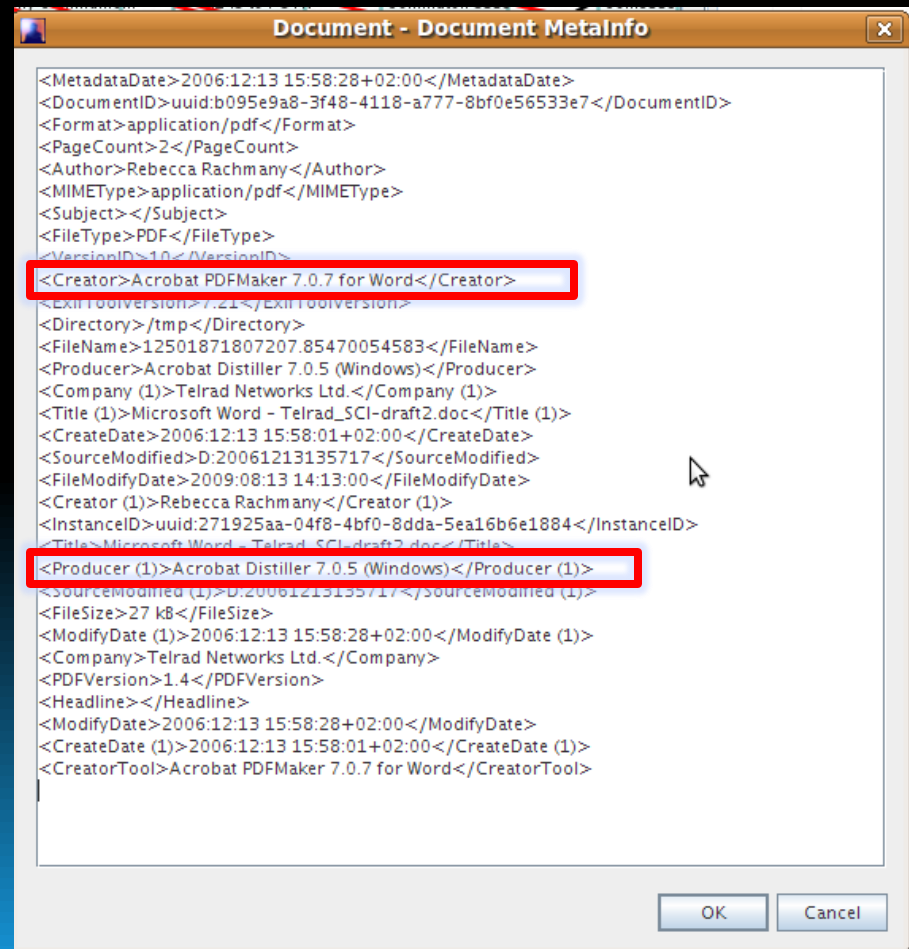
- Metadata to discover versions of software being used.

Important metadata:

```
mimetype - application/msword
language - U.S. English
paragraph count - 5
line count - 21
title - WINTER DRIVING TIPS
word count - 447
page count - 1
creator - JoynerD
date - 2009-03-03T13:23:00Z
generator - Microsoft Office Word
character count - 2552
last saved by - david.sanders3
creation date - 2009-03-03T13:23:00Z
template - Normal.dotm
```

Important metadata:

```
mimetype - application/vnd.ms-excel
creator - carterm
date - 2009-07-07T11:44:26Z
generator - Microsoft Excel
last saved by - richard.turrow
creation date - 2000-10-03T19:12:45Z
```



Document - Document MetaInfo

```
<MetadataDate>2006:12:13 15:58:28+02:00</MetadataDate>
<DocumentID>uuid:b095e9a8-3f48-4118-a777-8bf0e56533e7</DocumentID>
<Format>application/pdf</Format>
<PageCount>2</PageCount>
<Author>Rebecca Rachmany</Author>
<MIMETYPE>application/pdf</MIMETYPE>
<Subject></Subject>
<FileType>PDF</FileType>
<VersionID>1.0</VersionID>
<Creator>Acrobat PDFMaker 7.0.7 for Word</Creator>
<ExitToolVersion>7.21</ExitToolVersion>
<Directory>/tmp</Directory>
<FileName>12501871807207.85470054583</FileName>
<Producer>Acrobat Distiller 7.0.5 (Windows)</Producer>
<Company (1)>Telrad Networks Ltd.</Company (1)>
<Title (1)>Microsoft Word - Telrad_SCI-draft2.doc</Title (1)>
<CreateDate>2006:12:13 15:58:01+02:00</CreateDate>
<SourceModified>D:20061213135717</SourceModified>
<FileModifyDate>2009:08:13 14:13:00</FileModifyDate>
<Creator (1)>Rebecca Rachmany</Creator (1)>
<InstanceID>uuid:271925aa-04f8-4bf0-8dda-5ea16b6e1884</InstanceID>
<Title>Microsoft Word - Telrad_SCI-draft2.doc</Title>
<Producer (1)>Acrobat Distiller 7.0.5 (Windows)</Producer (1)>
<SourceModified (1)>D:20061213135717</SourceModified (1)>
<FileSize>27 kB</FileSize>
<ModifyDate (1)>2006:12:13 15:58:28+02:00</ModifyDate (1)>
<Company>Telrad Networks Ltd.</Company>
<PDFVersion>1.4</PDFVersion>
<Headline></Headline>
<ModifyDate>2006:12:13 15:58:28+02:00</ModifyDate>
<CreateDate (1)>2006:12:13 15:58:01+02:00</CreateDate (1)>
<CreatorTool>Acrobat PDFMaker 7.0.7 for Word</CreatorTool>
```

with 3 results

People / Organization: Document Metadata

- Office on Windows vs Office on Mac vs OpenOffice

```
user@titanium:~/Desktop$ extract madewithopenoffice3.0linux.ods
date - 2009-08-21T11:31:42
creation date - 2009-08-21T11:31:29
```

```
software - OpenOffice.org/3.0$Linux OpenOffice.org_project/300m15$Build-9379
```

```
mimetype - application/vnd.oasis.opendocument.spreadsheet
```

```
user@titanium:~/Desktop$
```

```
user@titanium:~/Desktop$
```

```
user@titanium:~/Desktop$ extract madewithopenoffice3.0linux.xls
```

```
mimetype - application/vnd.ms-office
```

```
date - 2009-08-21T15:31:42Z
```

```
creation date - 2009-08-21T15:31:29Z
```

```
user@titanium:~/Desktop$ █
```

```
user@titanium:~/Desktop$ extract madewithoffice2007win.xls
```

```
mimetype - application/vnd.ms-excel
```

```
creation date - 2009-08-21T15:40:04Z
```

```
generator - Microsoft Excel
```

```
creator - gatesjpl
```

```
last saved by - gatesjpl
```

```
date - 2009-08-21T15:40:50Z
```

```
user@titanium:~/Desktop$
```

```
user@titanium:~/Desktop$
```

```
user@titanium:~/Desktop$ extract madewithoffice2008mac.xls
```

```
mimetype - application/vnd.ms-files
```

```
creator - cg
```

```
date - 2009-08-21T15:36:17Z
```

```
generator - Microsoft Macintosh Excel
```

```
last saved by - cg
```

```
creation date - 2009-08-21T15:35:44Z
```

```
user@titanium:~/Desktop$ █
```

People / Organization: Document Metadata

- Issues.
 - Libextract sux for newer pdfs.

http://www.telrad.com/uploaded/press/Telrad_ArchitecturePatent_PR.pdf

Local copy [Open](#)

Important metadata:

```
Format - PDF 1.4
mimetype - application/pdf
```

- Ruby + pdf-parse can help us with that problem.
- FOCA too.

Telrad_ArchitecturePatent_PR.pdf

```
Creator=>"Acrobat PDFMaker 7.0.7 for Word",
_EmailSubject=>"MVNO",
Producer=>"Acrobat Distiller 7.0.5 (Windows)",
SourceModified=>"D20060907143303",
_AuthorEmailDisplayName=>"Itshak Aizner",
ModDate=>"D20060907173408+03'00'",
_AuthorEmail=>"itshak.aizner@telrad.com",
Title=>"For Immediate Release",
_AdHocReviewCycleID=>"-169073906",
CreationDate=>"D20060907173340+03'00'",
Company=>"Telrad Networks Ltd.",
_PreviousAdHocReviewCycleID=>"1049106379",
Author=>"Rebecca Rachmany"
```

People / Organization: Doc Metadata Tools

- Tools to get it done

- Maltego



MALTEGO²



- Metagoofil



Metagoofil

- PassiveRecon Firefox Plugin



PR

- FOCA



Goolag



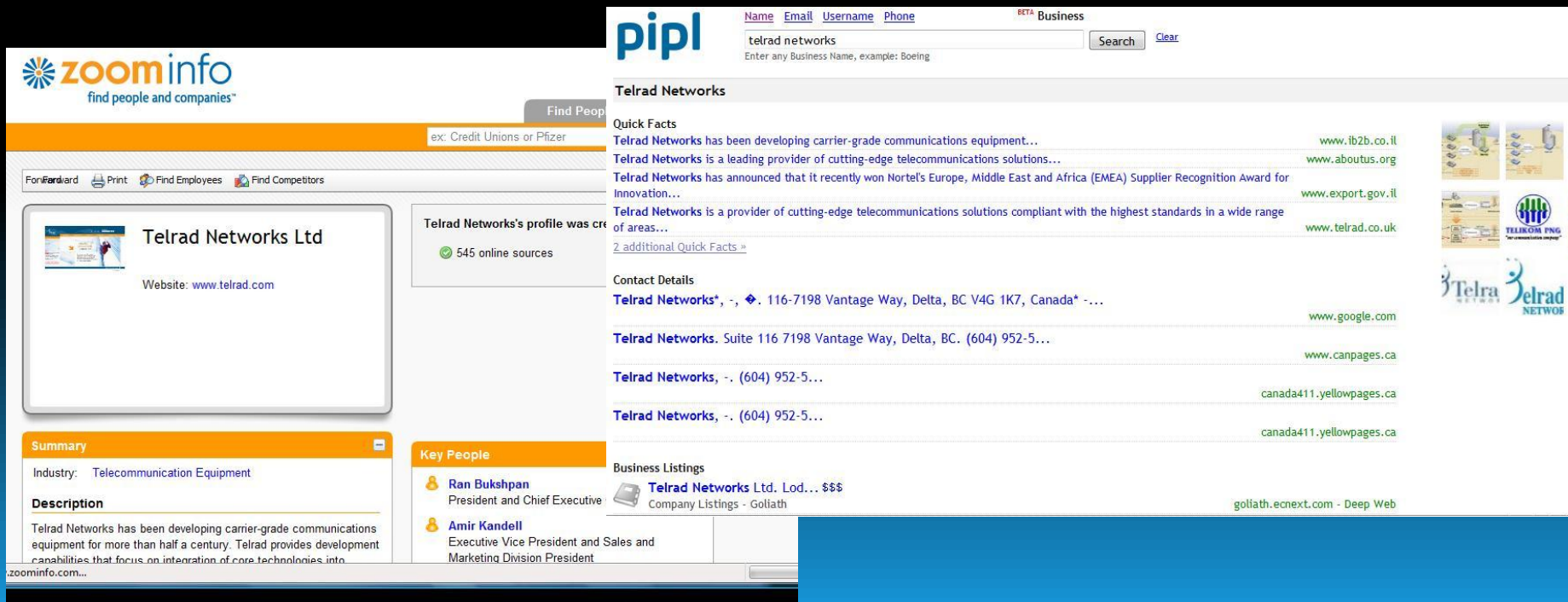
FOCA

- Goolag

- Roll your own with ruby & rubygem pdf-reader

People / Organization: Organization Profiling

- Online tools to find employees of companies
 - Most have APIs
 - Write your own tools to script infogathering
 - Write local transforms for Maltego



The image shows two overlapping web browser screenshots. The background screenshot is from ZoomInfo, displaying a profile for Telrad Networks Ltd. The foreground screenshot is from Pipl, showing search results for 'telrad networks'.

ZoomInfo Profile:

- Company:** Telrad Networks Ltd
- Website:** www.telrad.com
- Industry:** Telecommunication Equipment
- Description:** Telrad Networks has been developing carrier-grade communications equipment for more than half a century. Telrad provides development capabilities that focus on integration of core technologies into...
- Key People:**
 - Ran Bukshpan** - President and Chief Executive
 - Amir Kandell** - Executive Vice President and Sales and Marketing Division President

Pipl Search Results:

Search: telrad networks

Telrad Networks

Quick Facts

- Telrad Networks has been developing carrier-grade communications equipment... www.ib2b.co.il
- Telrad Networks is a leading provider of cutting-edge telecommunications solutions... www.aboutus.org
- Telrad Networks has announced that it recently won Nortel's Europe, Middle East and Africa (EMEA) Supplier Recognition Award for Innovation... www.export.gov.il
- Telrad Networks is a provider of cutting-edge telecommunications solutions compliant with the highest standards in a wide range of areas... www.telrad.co.uk

Contact Details

- Telrad Networks*, -, ♦. 116-7198 Vantage Way, Delta, BC V4G 1K7, Canada* -... www.google.com
- Telrad Networks, Suite 116 7198 Vantage Way, Delta, BC. (604) 952-5... www.canpages.ca
- Telrad Networks, -. (604) 952-5... canada411.yellowpages.ca
- Telrad Networks, -. (604) 952-5... canada411.yellowpages.ca

Business Listings

- Telrad Networks Ltd. Lod... \$\$\$ goliath.ecnext.com - Deep Web

People / Organization: Org Profiling Tools

- Tools to get it done

- Maltego
- Zoominfo
- Spoke
- Xing
- Spokeo
- 123people
- Pipl

MALTEGO²



 zoominfo
find people and companies™

XING 

spoke

spokeo™

pipl

123 people

People / Organization: People Profiling

- Handles are awesome and usually unique.

My friends call me

friendscall.me/YourName
organize your profiles in one place

Don't Let Squatters Get It.
we'll notify you of great new sites

Powerful Profiles
Analysis, Cleansing, Planning. ...an ounce of prevention...
www.travelautomation.net
[Access Private Profiles](#)
Access private profiles and photos on MySpac, Facebook, and 40+ sites!
www.spokeo.com
[Pimp My Profile](#)

namechk

Show All (130) Sort by Rank

Check to see if your desired *username* or *vanity url* is still available at dozens of popular Social Networking and Social Bookmarking websites. Promote your brand consistently by registering a username that is still available on the majority of the most popular sites. Find the best username with **namechk**.

✓ BackType Available	Facebook Maybe	LinkedIn Maybe	✓ Slide Available
✓ BallType Available	✓ Families.com Available	✓ LiveJournal Available	✓ Squidoo Available
✗ bebo Taken	✓ Fanpop Available	✓ Livevideo Available	✓ StumbleUpon Available
✓ Blip.fm Available	✗ Flickr Taken	✓ mixx Available	✗ Technorati Taken
✓ blip.tv Available	✓ Flixster Available	✓ Multiply Available	✓ ThisNext Available
✗ Blogger Taken	✗ FriendFeed Taken	✓ myLot Available	✓ tipd Available
✓ Buzznet Available	✓ funnyordie Available	✗ MySpace Taken	✓ Tribe Available
✓ cm cafemom Available	✓ Gather Available	✓ Netlog Available	✓ tumblr Available
✓ Current Available	✓ Good Reads Available	✓ newsvine Available	✗ Twitpic Taken
✓ DailyMotion Available	Google Maybe	✓ ning Available	✗ twitter Taken
✗ delicious Taken	✓ hi5 Available	✓ photobucket Available	✓ UStream Available
✓ deviantART Available	✓ Howcast Available	✓ PictureTrail Available	✓ Viddler Available
✗ Digg Taken	✓ Hulu Available	✓ Posterous Available	✓ Vimeo Available

Popular

Digg REGISTERED

Flickr AVAILABLE!

Etsy AVAILABLE!

LinkedIn REGISTERED

Pandora AVAILABLE!

FriendsCall.Me REGISTERED

Boing Boing REGISTERED

Facebook AVAILABLE!

Photo CHECK THIS CATEGORY

Flickr AVAILABLE!

Picasa AVAILABLE!

Webshots AVAILABLE!

People / Organization: People Profiling

- Handles are awesome and usually unique.

[advanced search](#)

Tweepz 1 - 2 of 2 for **indi303**

sort by: [relevancy](#) | [# followers](#) | [# following](#) | [join date](#)



indi303 (indi303)

followers: 417
following: 209
updates: 795
refreshed 1 day ago

[advanced search](#)

Tweepz 1 - 1 of 1 for **carnal0wnage**

sort by: [relevancy](#) | [# followers](#) | [# following](#) | [join date](#)



Chris Gates (carnal0wnage)

Evidently security isnt cool but i dont give a f**k
Location: NoVA
Web: <http://carnal0wnage.attackresearch.com>

followers: 1,161
following: 571
updates: 1,951
refreshed 2 days ago

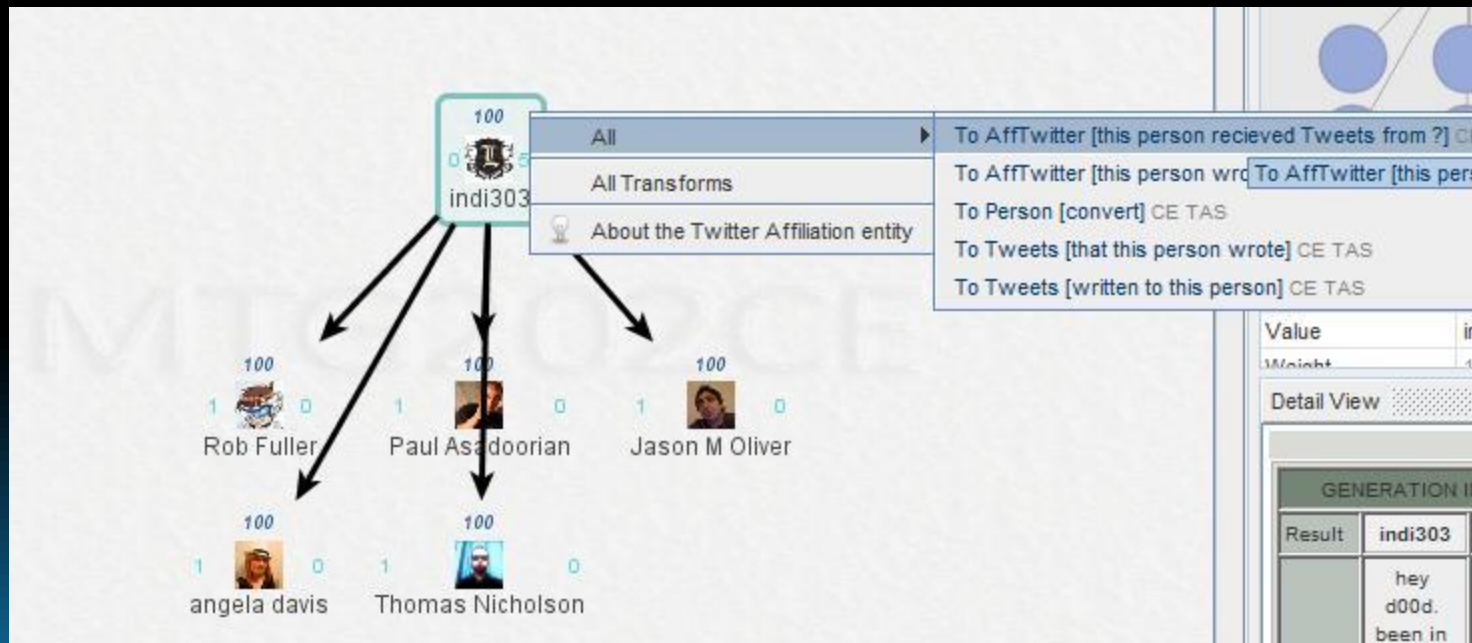
People / Organization: People Profiling

- Especially if you can turn them into twitter usernames or other social network profiles.



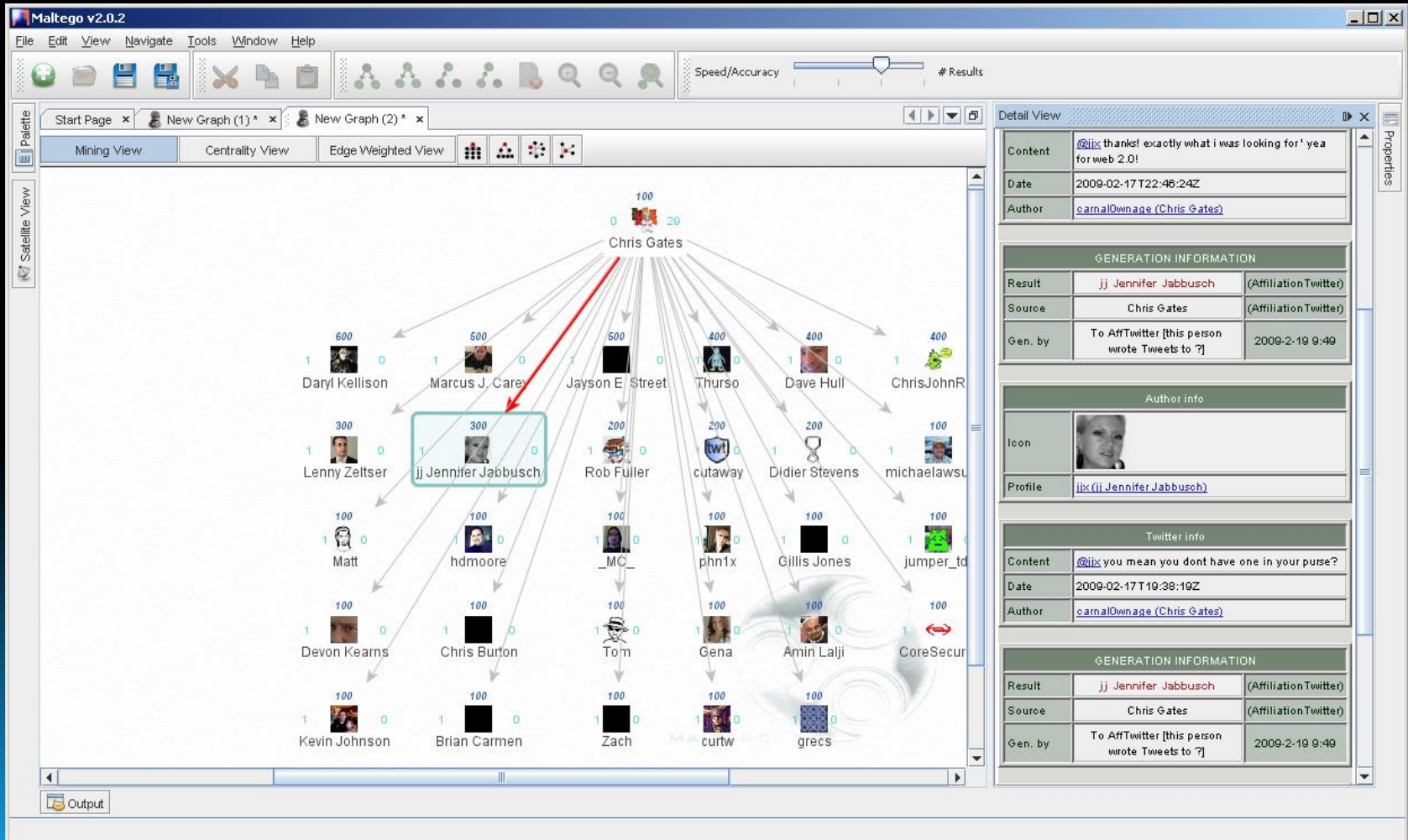
People / Organization: People Profiling

- Then we can see who they write tweets to and receive tweets from.



People / Organization: People Profiling

- Then we can see who they write tweets to and receive tweets from.



The screenshot shows the Maltego v2.0.2 interface. The main window displays a network graph with 'Chris Gates' at the top, connected to numerous other individuals. A red arrow points from Chris Gates to 'jj Jennifer Jabbusch', who is highlighted with a blue box. The detail view on the right shows two tweets from Chris Gates to jj Jennifer Jabbusch.

Maltego v2.0.2

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

Start Page x New Graph (1) * x New Graph (2) * x

Mining View Centrality View Edge Weighted View

Chris Gates (100) → Daryl Kellison (600), Marcus J. Carey (500), Jayson E. Street (500), Thurso (400), Dave Hull (400), ChrisJohnR (400), Lenny Zeltser (300), jj Jennifer Jabbusch (300), Rob Fuller (200), cutaway (200), Didier Stevens (200), michaelawsu (100), Matt (100), hdmoore (100), _MC_ (100), phn1x (100), Gillis Jones (100), jumper_td (100), Devon Kearns (100), Chris Burton (100), Tom (100), Gena (100), Amin Lalji (100), CoreSecur (100), Kevin Johnson (100), Brian Carmen (100), Zach (100), curtw (100), grecc (100)

Detail View

Content: @ix thanks! exactly what i was looking for 'yea for web 2.0!


Date: 2009-02-17 T22:46:24Z

Author: carnal0wnage (Chris Gates)

GENERATION INFORMATION

Result	jj Jennifer Jabbusch	(AffiliationTwitter)
Source	Chris Gates	(AffiliationTwitter)
Gen. by	To AffTwitter [this person wrote Tweets to ?]	2009-2-19 9:49

Author info

Icon: 

Profile: [ijx \(jj Jennifer Jabbusch\)](#)

Twitter info

Content: @ix you mean you dont have one in your purse?

Date: 2009-02-17 T19:38:19Z

Author: carnal0wnage (Chris Gates)

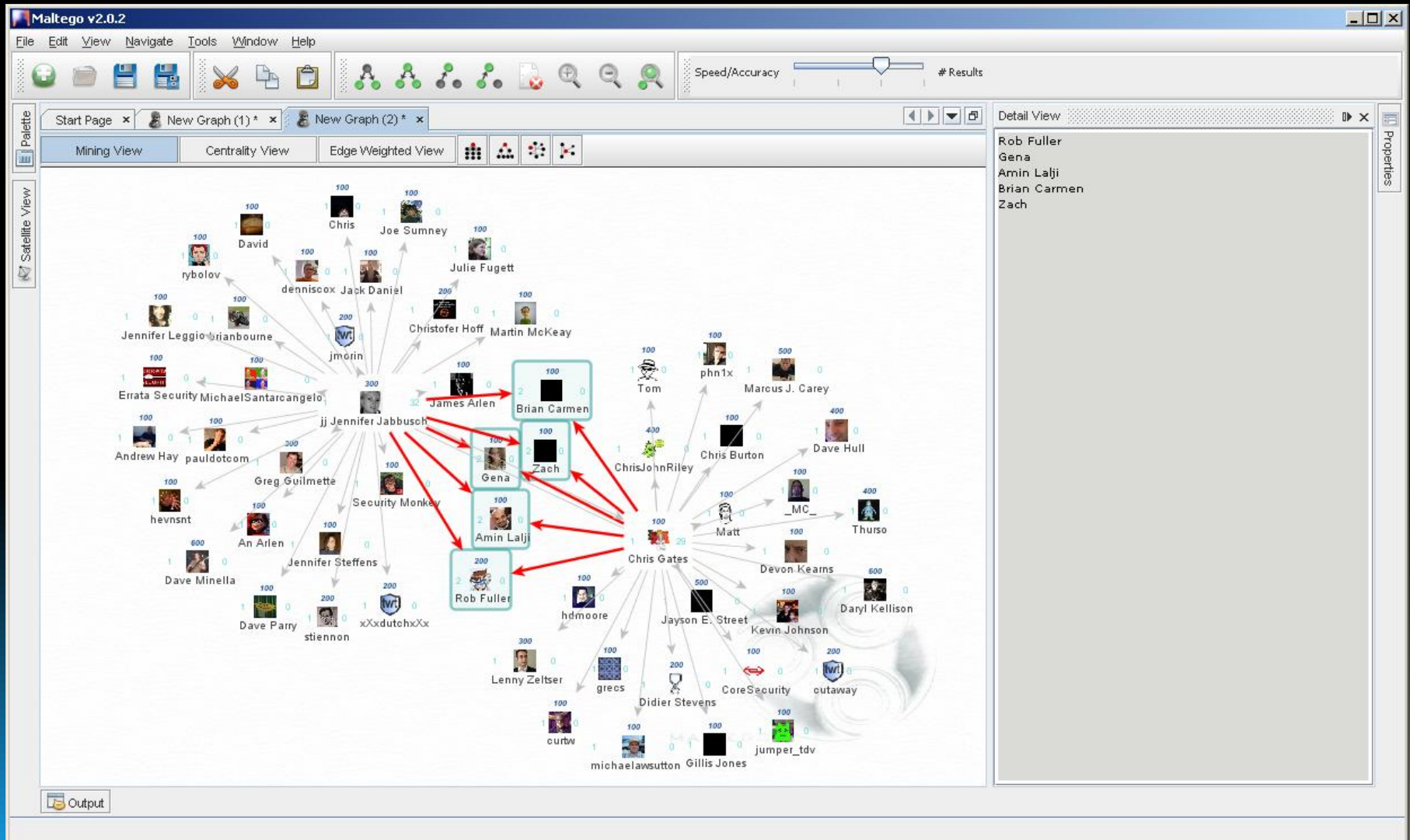
GENERATION INFORMATION

Result	jj Jennifer Jabbusch	(AffiliationTwitter)
Source	Chris Gates	(AffiliationTwitter)
Gen. by	To AffTwitter [this person wrote Tweets to ?]	2009-2-19 9:49

Output

People / Organization: People Profiling

- Then we can see who are common friends.




People / Organization: People Profiling

- Tons of information is placed into the public domain.






TweepSearch
About Help

In ur Tweeps, Crawl'n their Bioz!



Pro tip: Click on an avatar to limit the search to that person's followers.

Results: 1 - 20 of 54 for "bank of america". Sort by: last update ↑ | screen name ↓ | followers ↓ | friends ↓

This could be you! (@dacort on Twitter) - Seattle, WA Interested in having your profile here? Contact dacort [at] tweepsearch.com for more details in order to help TweepSearch grow. Reserve a keyword for \$10 for 30 days, or share with five others for \$5. <i>last recorded update about 1 awesome-second ago</i>			
	@BofA_help / David Knapp Bank of America - Phoenix, AZ futurebanking.bankofamerica...	Official Bank of America Twitter rep to help, listen and learn from our customers. To ensure privacy, never share account numbers in unsecured locations. <i>last recorded update 12 days ago</i>	followers: 3,034 friends: 1,057 updates: 1,818
	@mschiefmaker / Karen Biehl NYC www.TheCelebrityChihuahua.com	Owner of Eli the Celebrity Chihuahua, seen on the MilkBone box, FLN's Wingman, Queer Eye, Good Morning America , BET's Rip the Runway, Bank of America ads <i>last recorded update 11 days ago</i>	followers: 1,709 friends: 1,705 updates: 1,285
	@BankOAmericaSux / Bank of America Sux	<i>last recorded update 2 days ago</i>	followers: 1,517 friends: 1,466 updates: 925
	@DoryanCosta / Doryan Costa Warren, RI www.InternetLifestyleDreams...	I am a Bank of America Manager, and Internet Marketer...Helping You Make Money At Home..and Helping you Deposit It and Keep It Safe :) <i>last recorded update about 1 hour ago</i>	followers: 5,961 friends: 5,717 updates: 269
	@LynnSaratore / Lynn Saratore Chicago www.linkedin.com/in/lynnsar...	HR Generalist at CDW, previously Sr. Recruiter @ Hewitt and Staffing Manager @ Bank of America <i>last recorded update 20 days ago</i>	followers: 335 friends: 465 updates: 78







People / Organization: People Profiling

- Tons of information is placed into the public domain.

TweepSearch BETA

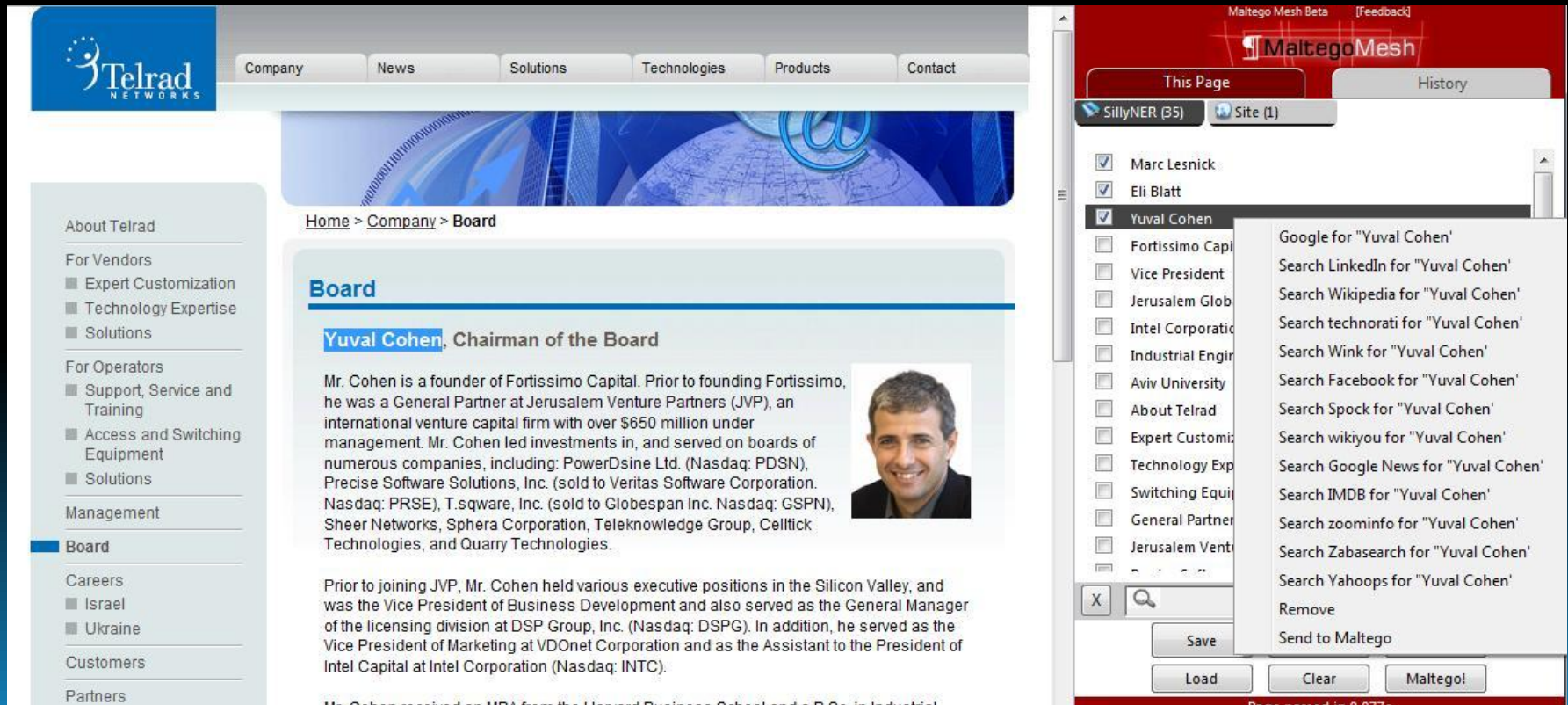
Pro tip: Click on an avatar to limit the search to that person's followers.

Results: 1 - 20 of 1,118 for cisco. Sort by: [last update](#) ↓ | [screen name](#) ↓ | [followers](#) ↑ | [friends](#) ↓

<p>This could be you! (@dacort on Twitter) - Seattle, WA Interested in having your profile here? Contact dacort [at] tweepsearch.com for more details in order to help TweepSearch grow. Reserve a keyword for \$10 for 30 days, or share with five others for \$5. <i>last recorded update about 1 awesome-second ago</i></p>			
	<p>@Padmasree / Padmasree California</p>	<p>CTO of Cisco <i>last recorded update 3 months ago</i></p>	<p>followers: 410,345 friends: 66 updates:</p>
	<p>@CiscoSystems / Cisco Systems Silicon Valley blogs.cisco.com/news/</p>	<p>News and info about Cisco, our CEO and execs. I am @John_Earnhardt and am your tourguide on our official Twitter feed. Cisco Support @ http://www.cisco.com/tac <i>last recorded update 12 days ago</i></p>	<p>followers: 13,506 friends: 2,455 updates: 1,248</p>
	<p>@GlobalKnowledge / Global Knowledge Worldwide www.globalknowledge.com</p>	<p>Worldwide Leader in IT and Business Training, focusing on Cisco, Microsoft, and Project Management. www.globalknowledge.com <i>last recorded update about 12 hours ago</i></p>	<p>followers: 13,977 friends: 7,391 updates: 956</p>
	<p>@fableton / Leonard Fableton twitter leonardfableton.com</p>	<p>my kids are named whiteport, wild irish rose, seagrams 7, old style classic draft, cisco, and mad dog2020 <i>last recorded update 3 months ago</i></p>	<p>followers: 7,708 friends: 7,665 updates: 4,787</p>
	<p>@Cisco_X1Concept / Cisco Kuala Lumpur www.x1concept.com/blog</p>	<p>Founder X1Concept Network Marketing and Internet Marketing Fan Health Freak and Supplement Evangelist, Harley Fan, Reader, Listener, Entrepreneur <i>last recorded update 2 days ago</i></p>	<p>followers: 6,842 friends: 7,298 updates: 582</p>
	<p>@jessicalearning / Jessica Duncan California www.linkedin.com/in/jessica...</p>	<p>Social media fan, RPG video game enthusiast, training professional, Cisco employee, Kindle owner, running and fitness addict, and lover of new technology <i>last recorded update 4 days ago</i></p>	<p>followers: 6,733 friends: 6,611 updates: 1,238</p>

People / Organization: People Profiling

- Tons of information is placed into the public domain.



The image shows a screenshot of a corporate website for Telrad Networks, specifically the 'Board' page. The profile for Yuval Cohen, Chairman of the Board, is displayed. A Maltego search interface is overlaid on the right side of the page, showing a search for 'Yuval Cohen' with various search engines and filters selected. The Maltego interface includes a search bar, a list of search engines, and a 'Save' button.

Telrad Networks Website Content:

- Navigation: Company, News, Solutions, Technologies, Products, Contact
- Page Title: Home > Company > Board
- Section: **Board**
- Profile: **Yuval Cohen, Chairman of the Board**
- Description: Mr. Cohen is a founder of Fortissimo Capital. Prior to founding Fortissimo, he was a General Partner at Jerusalem Venture Partners (JVP), an international venture capital firm with over \$650 million under management. Mr. Cohen led investments in, and served on boards of numerous companies, including: PowerDsine Ltd. (Nasdaq: PDSN), Precise Software Solutions, Inc. (sold to Veritas Software Corporation. Nasdaq: PRSE), T.square, Inc. (sold to Globespan Inc. Nasdaq: GSPN), Sheer Networks, Sphera Corporation, Teleknowledge Group, Celltick Technologies, and Quarry Technologies.
- Additional Info: Prior to joining JVP, Mr. Cohen held various executive positions in the Silicon Valley, and was the Vice President of Business Development and also served as the General Manager of the licensing division at DSP Group, Inc. (Nasdaq: DSPG). In addition, he served as the Vice President of Marketing at VDonet Corporation and as the Assistant to the President of Intel Capital at Intel Corporation (Nasdaq: INTC).

Maltego Search Interface:

- Search Term: Yuval Cohen
- Selected Search Engines: Marc Lesnick, Eli Blatt, Yuval Cohen, Fortissimo Capital, Vice President, Jerusalem Glob, Intel Corporat, Industrial Engir, Aviv University, About Telrad, Expert Customiz, Technology Exp, Switching Equip, General Partner, Jerusalem Vent
- Search Options: Google for "Yuval Cohen", Search LinkedIn for "Yuval Cohen", Search Wikipedia for "Yuval Cohen", Search technorati for "Yuval Cohen", Search Wink for "Yuval Cohen", Search Facebook for "Yuval Cohen", Search Spock for "Yuval Cohen", Search wikiyou for "Yuval Cohen", Search Google News for "Yuval Cohen", Search IMDB for "Yuval Cohen", Search zoominfo for "Yuval Cohen", Search Zabasearch for "Yuval Cohen", Search Yahoops for "Yuval Cohen", Remove, Send to Maltego
- Buttons: Save, Load, Clear, Maltego!

People / Organization: People Profiling Tools

- Tools to get it done

- Maltego
- Maltego Mesh
- knowem.com
- friendscall.me
- namechk.com
- usernamecheck.com
- tweepz.com
- tweepsearch.com



MALTEGO²



knowem?
thwart social media identity theft



Friends call me...



namechk



tweepz

Look who's tweeting



TweepSearch
BETA

Final Considerations

- If someone doesn't have strong Internet presence can I become them?
 - Create gmail accounts.
 - Register them on LinkedIn.
 - Skype/Gtalk/MSN/be them on IRC or SILC.
 - Register them on Facebook/Myspace/Twitter/etc.
 - Create their blog.
- Or can I create a company employee and “make new friends”?

... AUTOMATED



Virtual Identity creator

How many identities? ID store:
Names file

Social networks

- FaceBook
- LinkedIn
- Bebo
- MySpace
- Twitter
- Orkut
- Random

Email Address

- Gmail
- Inbox
- Yahoo
- Hotmail

Blogs

- Blogspot
- Wordpress
- Random

THIS APP DOES NOT REALLY EXIST!!

Maint

Activity Tempa 12h 24h 36h 48h 72h 240h

- Post
- Action
- Comment
- Random

ID file

Debugging info

- 1.1 Building email adutre
kosie.kramer1@gmail.co
kosiek@yahoo.com - ple
kramerks@hotmail.com
- 1.2 Building Social netw
KosieKramer at FaceBoo
kosie.kramer@gmail.co
KosieKramer at Orkut v
- 1.3 Building blogs
kosiekramerblog.blogspot.com with Gmail addr
kosiescool.wordpress.com with Yahoo email ad

Setting Action on ID1 (Kosie Kramer) to "Working" for [Facebook]
Setting Comment for ID1 (Kosie Kramer) on <http://sample.blogspot.comcomment.g?blogID=113402209033317>
Setting Action on ID4 (Mark Soap) to "Out to lunch" for [Twitter]
Setting Post on ID3 (John Breda) to "After the collapse of the Roman empire the pipes remained a popular instrum
Setting Comment for ID2 (Peter Muller) on <http://security.wordpress.com/2005/10/22/openbsds-network-stack>
Setting Comment for ID4 (Mark Soap) on <http://eatwhatyoufeed.wordpress.com/2007/02/18/freerange-chicker>

Progress

Waiting for captchas to complete
DONE - Identity 1: stored in c:\identities.txt

05/ABB

Up next Chris Nickerson



To tell you what to do with
all that IG goodness...

Educate Yourself

- Useful Resources

- Paterva

- Maltego. Go Buy It!

- <http://www.paterva.com/web4/index.php/media/presentations>

- Christian Martorella (Edge-Security)

- <http://laramies.blogspot.com/>

- <http://www.edge-security.com/presentations.php>

- Larry Pesche

- Document Metadata, the Silent Killer

- P2P Information Disclosure

- Rob Fuller (mubix)

- <http://www.room362.com/>

Thank You!

Questions?