

A fresh new look into Information Gathering



Christian Martorella
IV OWASP MEETING SPAIN



S21sec
Tomorrow's Digital Security, Today

Who am i ?

Christian Martorella

- Manager Auditoria S21sec
- CISSP, CISA, CISM, OPST, OPSA
- OWASP WebSlayer Project Leader
- OISSG, Board of Directors
- FIST Conference, Presidente
- Edge-Security.com

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.”

OSINT: Open Source INTelligence

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

Penetration test anatomy

Information Gathering

Discovery / Fingerprinting

Vulnerability analysis

Exploitation

Reporting

Types of I.G

Passive

Active

I.G - Types of information

- Domain, subdomain/host names ➔ **dev.target.com**
- User names ➔ **jdoe**
- Email Accounts ➔ **jdoe@target.com**
- Person names ➔ **John Doe**

I.G what for?

- Infraestructure:
 - Information for discovering new targets, to get a description of the hosts (NS,MX, AS,etc), shared resources
- People and organizations:
 - For performing brute force attacks on available services, Spear phishing, social engineering, investigations, analysis, background checks, information leaks

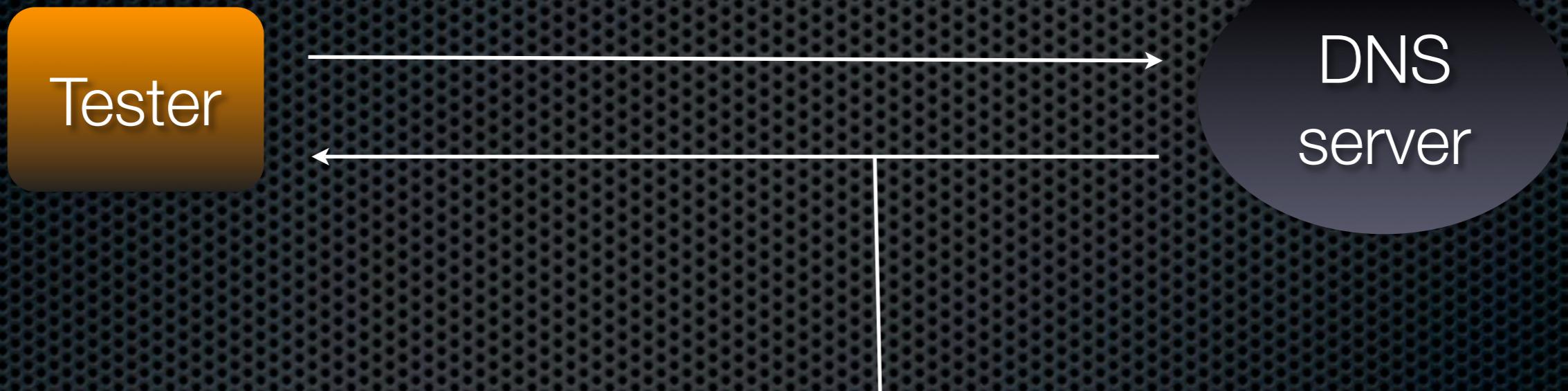
How can we obtain this kind
of info?

Obtaining host and Domains info - Classic

- Zone Transfer (active)
- Whois (passive)
- Reverse Lookup (active)
- BruteForce (active++)
- Mail headers (active)
- smtp (active++)

Zone-Transfer - DIG

request: dig @srv.weak.dns weak.dns -t AXFR

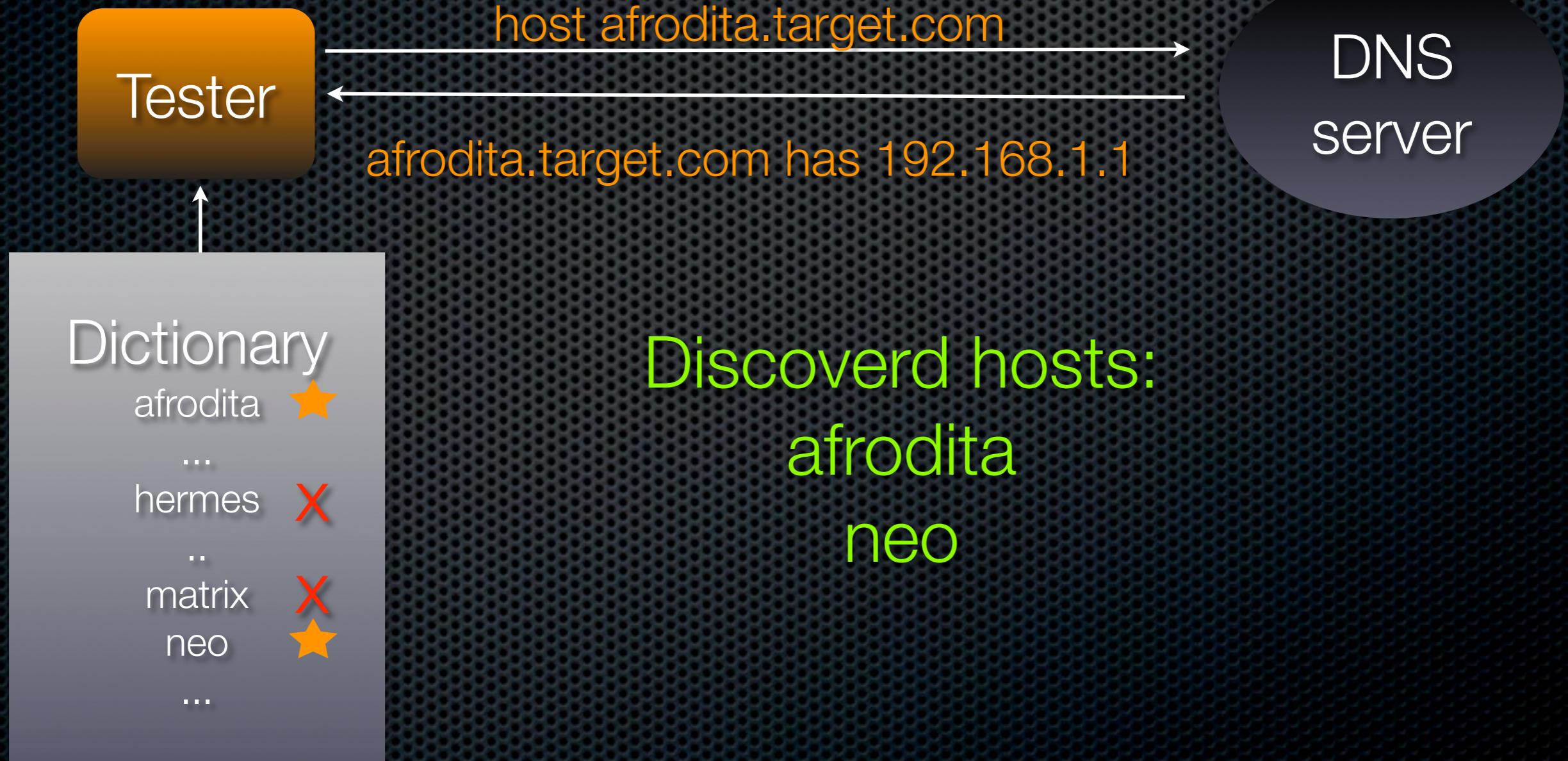


```
brad@rt001:/root$ dig @srvr.weak.dns -t AXFR weak.dns

; <>> DiG 9.2.4 <>> @srvr.weak.dns -t AXFR weak.dns
;; global options: printcmd
weak.dns.      3600   IN      SOA    ns.weak.dns. hostmaster.weak.dns. 2005061602
3600 900 600000 3600
weak.dns.      3600   IN      NS     ns.weak.dns.
weak.dns.      3600   IN      NS     ns2.weak.dns.
weak.dns.      3600   IN      NS     some.weak.dns.
weak.dns.      3600   IN      NS     other.weak.dns.
weak.dns.      3600   IN      MX     10 mail-in.weak.dns.
weak.dns.      3600   IN      MX     200 relay1.weak.dns.
weak.dns.      3600   IN      A      x.x.x.x
filer0-501.weak.dns. 3600 IN      A      x.x.x.x
xxx-xx-xxx-xx.weak.dns. 3600 IN      A      x.x.x.x
xxx-xx-xxx-xx.weak.dns. 3600 IN      A      x.x.x.x
```

DNS bruteforce

Domain: target.com



Mail Headers

```
Received: from smtp.example.com (6.Net-45-12-192.dynamicIP.example.net  
[192.12.45.6])  
        by mail.example.org (Postfix) with ESMTP id 0AB0E147B1  
  
Received: from smtp.example.com (smtp.example.com [172.18.5.21])  
        by mx1.example.com (8.11.6/8.11.6) with ESMTP id i82sokwis;  
  
Received: from vaio (172.16.1.100)  
        by smtp.example.com (Postfix) with ESMTP id i82shwk;
```

X-Mailer: Microsoft office outlook, Build 11.0.5510

User-Agent: Thunderbird 1.5.0.7 (Windows/20060909)

X-Mailer: ColdFusion MX Application Server

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2962

X-Mailer: Evolution 2.2.3 (2.2.3-4.fc4)

X-Mailer: iPlanet Messenger Express 5.2 Patch 2 (built Jul 14 2004)

Obtaining user info - Classic

- Search engines (passive)
- Web pages (active)



New sources for I.G ...

Obtaining host and Domains info

- Search Engines (passive)
- Public PGP key servers (passive)
- serversniff.net and others (passive)

Obtaining host and Domains - Search engines

Passive

"nasa.gov" – Buscar con Google

http://www.google.es/search?hl=es&q="nasa.gc... ▾

capture video free

Acceder

La Web Imágenes Noticias Maps ¡Nuevo! Grupos Más »

"nasa.gov"

Buscar Búsqueda avanzada Preferencias

Búsqueda: la Web páginas en español páginas de España

La Web Resultados 1 - 10 de aproximadamente 13.100.000 de "nasa.gov". (0,04 segundos)

[NASA - Home](#) - [Traduzca esta página]

The nasa.gov site requires that JavaScripts be enabled in your browser. ... Follow this link to go to the text only version of nasa.gov ...

[www.nasa.gov/](#) - 69k - En caché - Páginas similares

[Space Shuttle](#) [STEREO - The Sun in 3D](#)
[MULTIMEDIA](#) [Results](#)
[News - Highlights](#) [Want to Work at NASA?](#)
[Missions - Highlights](#) [Space Station Section](#)

[Más resultados de nasa.gov »](#)

[Ciencia @ NASA](#)

Reportajes científicos sobre astronomía, ciencias espaciales, física y biología.

[ciencia.nasa.gov/](#) - 17k - En caché - Páginas similares

[El Sol se volteó](#)

Actualizaciones sobre la misión de la sonda Ulises se pueden encontrar en Internet por el JPL en <http://ulysses.jpl.nasa.gov>. ...

[ciencia.nasa.gov/headlines/y2001/ast15feb_1.htm](#) - 19k - En caché - Páginas similares
[Más resultados de ciencia.nasa.gov]

[Imágenes Interactivas de Satélites Meteorológicos Geoestacionarios ...](#)

Oficial Responsable: Dr. James E. Arnold (jim.arnold@msfc.nasa.gov) Administrador de la Página: Paul J. Meyer (paul.meyer@msfc.nasa.gov) ...

[weather.msfc.nasa.gov/GOES/goes_es.html](#) - 12k - En caché - Páginas similares

[The Space Place :: Inicio](#)

Informaciones, juegos, entretenimientos y curiosidades sobre el mundo espacial.

[spaceplace.nasa.gov/sp/kids/](#) - 18k - En caché - Páginas similares

[Exploración de Marte: Reseña general](#)

El sol detrás del limbo de Marte Desde nuestra primera foto detallada de Marte tomada en 1965, viajes de sonda espaciales al planeta rojo han revelado un

subdomain

Obtaining host and Domains info



The PGP public key servers are only intended to help the user in exchanging public keys

<http://keyserver.veridis.com/>

[http://pgp.rediris.es:11371/pks/lookup?
search=domain](http://pgp.rediris.es:11371/pks/lookup?search=domain)

Obtaining host and Domains info

OpenPGP Keyserver - search for keys

<http://keyserver.veridis.com:11371/search?q=apple.com&p=3>

KeyServer @veridis.com

Import

Results 63 - 93 of about 555 for apple.com. (0.044 seconds)

Key(s)	Key ID	Size	Creation	Expiration
▶ Brian Maggi <maggi@apple.com>	0xE490FA1A	2048/1024	1999/10/22	Never
▶ Brian Maggi <maggi@apple.com>	0xBF99BA50	1024	1999/02/04	2001/02/04
▶ Brian R. Smiley <bsmiley@apple.com>	0x4720B5A4	2048/1024	1998/11/06	Never
▶ Brian Smiley <bsmiley@apple.com>	0xF58C579E	2048/1024	1998/07/27	Never
▶ Brian Washburn <brian@may-apple.com>	0x35976A31	2048/1024	2005/12/07	Never
▶ Bruce Thompson (work RSA) <bruce@newton.apple.co	0xB072B089	2048	1997/07/21	Never
▶ Bruce Thompson (Work) <bruce@newton.apple.com>	0x7F6C922D	2048/1024	1997/07/21	Never
✖ Bruce Thompson (obsolete)	0xD3B76181	1024	1997/04/04	Never
▶ Byron Han <han@hanchenson.com>	0xE1C07332	3072/1024	1997/10/24	Never
▶ c.repair <c.repair@asia.apple.com>	0x34B77C7A	2048/1024	2001/04/18	Never
▶ Cameron Esfahani <dirty@apple.com>	0x1283E49C	1024	1998/11/26	Never
▶ Carlos Espana <cespana@apple.com>	0x2B2E7F4B	2048/1024	2001/02/27	Never
▶ CCS <ccsi@asia.apple.com>	0xA45BCE3D	1024	1998/03/17	Never
▶ Chad Lawson <cdlawson@apple.com>	0xF7907F08	1024/1024	2002/04/11	Never
▶ Chad Williams <chad@apple.com>	0x8820BF7B	4096/1024	1998/06/05	Never
▶ Charles Vollum <moana@xsw.com>	0x8000BF0C9	1024	1993/11/23	Never
▶ Charles Evans <cevans@apple.com>	0xD928A7BF	1024/1024	1999/05/31	Never
✖ Charles Wiltgen <cwiltgen@apple.com>	0xB54C53C1	2048/1024	1997/06/02	Never
✖ Chris A. Gorden <cgagg@interlog.com>	0x7508B5C3	512	1993/05/17	Never
▶ Chris Bourdon <bourdon@apple.com>	0x85E0CE9E	1024/1024	1999/11/20	Never
✖ Chris De Salvo <desalvo@apple.com>	0xC0AAEC45	2048	1997/08/01	Never
✖ Chris De Salvo <desalvo@apple.com>	0xD881007E	2048/1024	1997/07/23	Never
▶ Chris De Salvo <desalvo@apple.com>	0xBA597DFS	1024	1996/12/17	Never
▶ Chris Jalbert <jalbert@apple.com>	0x802B27EB	2048/1024	1997/09/11	Never
▶ Chris Rives <grumpus@apple.com>	0x12449B78	2048/1024	1999/09/30	Never
▶ Chris Rudolph <chris_rudolph@apple.com>	0x1BDA1A80	2048/1024	1998/05/22	Never
▶ Chris Rudolph <chris_rudolph@apple.com>	0x18C0A51C	2048/1024	1998/05/21	Never
▶ Chris Rudolph <chris_rudolph@apple.com>	0x28BA1004	2048/1024	1998/05/21	Never
▶ Chris Spalding <cls@apple.com>	0x5E4BEF9B	2048/1024	1999/09/09	Never
▶ Christian Hillcoat <hillcoat.c@euro.apple.com>	0x19DF4661	4096/1024	1999/11/25	Never
▶ Christian van der Leeden <leeden@euro.apple.com>	0x053DFD01	2048	2000/09/11	Never

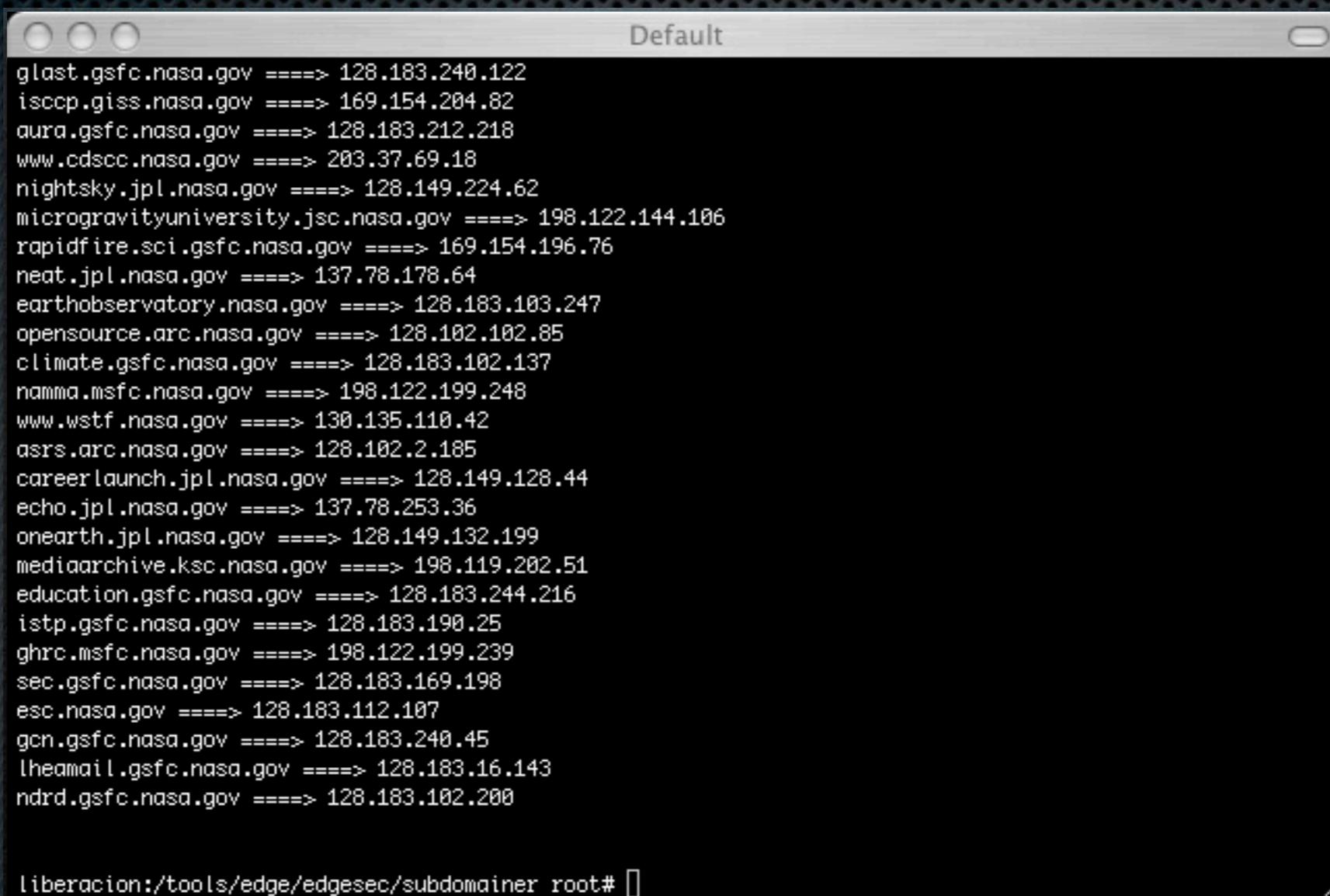
Page 3 of 18

F.A.Q.

Send bugs and comments to keymaster@veridis.com

subdomains

Obtaining host and Domains Subdomainer



The screenshot shows a terminal window titled "Default" displaying a list of domain mappings. Each entry consists of a domain name followed by a double arrow (====>) and its corresponding IP address. The domains listed are: glast.gsfc.nasa.gov, isccp.giss.nasa.gov, aura.gsfc.nasa.gov, www.cdscc.nasa.gov, nightsky.jpl.nasa.gov, microgravityuniversity.jsc.nasa.gov, rapidfire.sci.gsfc.nasa.gov, neat.jpl.nasa.gov, earthobservatory.nasa.gov, opensource.arc.nasa.gov, climate.gsfc.nasa.gov, namma.msfc.nasa.gov, www.wstf.nasa.gov, asrs.arc.nasa.gov, careerlaunch.jpl.nasa.gov, echo.jpl.nasa.gov, onearth.jpl.nasa.gov, mediaarchive.ksc.nasa.gov, education.gsfc.nasa.gov, istp.gsfc.nasa.gov, ghrc.msfc.nasa.gov, sec.gsfc.nasa.gov, esc.nasa.gov, gcn.gsfc.nasa.gov, theamail.gsfc.nasa.gov, and ndrd.gsfc.nasa.gov. The terminal prompt at the bottom indicates the user is root.

```
glast.gsfc.nasa.gov =====> 128.183.240.122
isccp.giss.nasa.gov =====> 169.154.204.82
aura.gsfc.nasa.gov =====> 128.183.212.218
www.cdscc.nasa.gov =====> 203.37.69.18
nightsky.jpl.nasa.gov =====> 128.149.224.62
microgravityuniversity.jsc.nasa.gov =====> 198.122.144.106
rapidfire.sci.gsfc.nasa.gov =====> 169.154.196.76
neat.jpl.nasa.gov =====> 137.78.178.64
earthobservatory.nasa.gov =====> 128.183.103.247
opensource.arc.nasa.gov =====> 128.102.102.85
climate.gsfc.nasa.gov =====> 128.183.102.137
namma.msfc.nasa.gov =====> 198.122.199.248
www.wstf.nasa.gov =====> 130.135.110.42
asrs.arc.nasa.gov =====> 128.102.2.185
careerlaunch.jpl.nasa.gov =====> 128.149.128.44
echo.jpl.nasa.gov =====> 137.78.253.36
onearth.jpl.nasa.gov =====> 128.149.132.199
mediaarchive.ksc.nasa.gov =====> 198.119.202.51
education.gsfc.nasa.gov =====> 128.183.244.216
istp.gsfc.nasa.gov =====> 128.183.190.25
ghrc.msfc.nasa.gov =====> 198.122.199.239
sec.gsfc.nasa.gov =====> 128.183.169.198
esc.nasa.gov =====> 128.183.112.107
gcn.gsfc.nasa.gov =====> 128.183.240.45
theamail.gsfc.nasa.gov =====> 128.183.16.143
ndrd.gsfc.nasa.gov =====> 128.183.102.200

liberacion:/tools/edge/edgesec/subdomainer root# []
```

Obtaining host and Domains Subdomainer

Once we have some host names, we can improve our dictionary using Google sets, and then try a brute force attack on the dns.

Obtaining host and Domains Subdomainer

[Feedback](#) [Discuss](#) [Terms of Use](#)

Google Sets™

Automatically create sets of items from a few examples.

Enter a few items from a set of things. ([example](#))
Next, press *Large Set* or *Small Set* and we'll try to predict other items in the set.

-
-
-
-
-

[\(clear all\)](#)

[Large Set](#) [Small Set \(15 items or fewer\)](#)

[Feedback](#) [Discuss](#) [Terms of Use](#)

Google Sets™

Predicted Items

- [saruman](#)
- [frodo](#)
- [bilbo](#)
- [gandalf](#)
- [legolas](#)
- [gimli](#)
- [aragorn](#)
- [gollum](#)
- [boromir](#)
- [galadriel](#)
- [arwen](#)
- [elrond](#)
- [sam](#)
- [merry](#)
- [pippin](#)
- [faramir](#)
- [sauron](#)
- [eowyn](#)
- [theoden](#)
- [eomer](#)
- [denethor](#)

WikiScanner

- Company IP ranges
- Anonymous Wikipedia edits, from interesting organizations
- <http://wikiscanner.virgil.gr/>

WikiScanner - IP ranges

Found 150 IP ranges for 'bank of america'

Your query returned more than 150 results, but we're only showing the first 150 for efficiency reasons. -Virgil

	IP Range	Name	Domain	Location	EN edits	DE edits	JA Edits
<input type="checkbox"/>	171.159.129.0-160.231.255	Bank Of America	pacbell.net [web]	Concord, California, United States	1396	1	0
<input type="checkbox"/>	171.161.160.0-255	Bank Of America	pacbell.net [web]	Dallas, Texas, United States	990	8	0
<input type="checkbox"/>	171.159.64.0-255	Bank Of America	pacbell.net [web]	Walnut Creek, California, United States	827	1	0
<input type="checkbox"/>	171.161.224.0-255	Bank Of America	bankofamerica.com [web]	Charlotte, North Carolina, United States	605	0	0
<input type="checkbox"/>	171.191.65.0-196.96.255	Bank Of America	pacbell.net [web]	Concord, California, United States	223	0	0
<input type="checkbox"/>	171.161.96.0-255	Bank Of America	bankofamerica.com [web]	Pasadena, California, United States	199	0	0
<input type="checkbox"/>	171.158.6.0-159.63.255	Bank Of America	davita.com [web]	Concord, California, United States	103	38	0
<input type="checkbox"/>	171.160.233.0-161.95.255	Bank Of America	pacbell.net [web]	Concord, California, United States	82	0	0
<input type="checkbox"/>	171.159.128.0-255	Bank Of America	bankofamerica.com [web]	Chicago, Illinois, United States	22	0	0
<input type="checkbox"/>	63.148.5.0-63	Woori America Bank	qwest.net [web]	Flushing, New York, United States	19	0	0
<input type="checkbox"/>	206.229.105.0-63	First National Bank Of America	-	East Lansing, Michigan, United States	14	0	0
<input type="checkbox"/>	69.208.102.112-119	Mid America Bank	-	Chicago, Illinois, United States	9	0	0

WikiScanner - Wikipedia edits

Found 22 edits within
171.159.128.0-255

Submit your favorite edits to Wired's [27bstroke6](#).

ip	title	diff	comment	time
171.159.128.10	1974 in film <small>[cur]</small>	5080980	<small>/* Other Movies Released */</small>	2004-07-14 13:33:06
171.159.128.10	Bosch reaction <small>[cur]</small>	4928021		2004-06-25 14:10:03
171.159.128.10	Evangelical Lutheran Synod <small>[cur]</small>	13907709	<small>/* History */</small>	2005-03-30 16:13:13
171.159.128.10	Fencing <small>[cur]</small>	4821554	<small>/* Notable modern fencers and fencing masters */</small>	2004-07-23 19:18:12
171.159.128.10	IBM Rational ClearCase <small>[cur]</small>	4260457		2004-06-24 17:54:29
171.159.128.10	Lutheranism <small>[cur]</small>	11739455	<small>/* Denomination organization */</small>	2005-03-30 15:57:53
171.159.128.10	MediaWiki talk:Recentchangestext <small>[cur]</small>	4021222	<small>/* Requested Articles */</small>	2004-06-10 18:13:44
171.159.128.10	MOD (file format) <small>[cur]</small>	7042652	<small>/* Software */</small>	2004-09-21 15:54:12
171.159.128.10	Prior art <small>[cur]</small>	5147269	<small>/* First-to-file systems */</small>	2004-08-11 18:38:52
171.159.128.10	Terraforming <small>[cur]</small>	4262808		2004-06-24 19:46:46
171.159.128.10	Terraforming <small>[cur]</small>	4263486	<small>/* Converting atmosphere */</small>	2004-06-24 19:54:23
171.159.128.10	Terraforming <small>[cur]</small>	4264445	<small>/* In fiction */</small>	2004-06-24 21:25:47
171.159.128.10	Terraforming <small>[cur]</small>	4264707	<small>/* History */</small>	2004-06-24 21:45:24
171.159.128.10	Terraforming <small>[cur]</small>	4264749	<small>/* Ethical issues */</small>	2004-06-24 21:50:27
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810524		2004-07-23 22:17:46
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810537		2004-07-23 22:18:46
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810548		2004-07-23 22:19:58
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810611		2004-07-23 22:20:51
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810820		2004-07-23 22:25:38
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810835		2004-07-23 22:35:51
171.159.128.10	Vladimir Nazlymov <small>[cur]</small>	4810984		2004-07-23 22:36:34
171.159.128.10	Wikipedia:Introduction <small>[cur]</small>	13800404		2005-05-16 20:29:48

Obtaining user info - New sources

- PgP key servers (passive)
- Social Networks (passive)
- Metadata (passive)

Obtaining user info - New sources

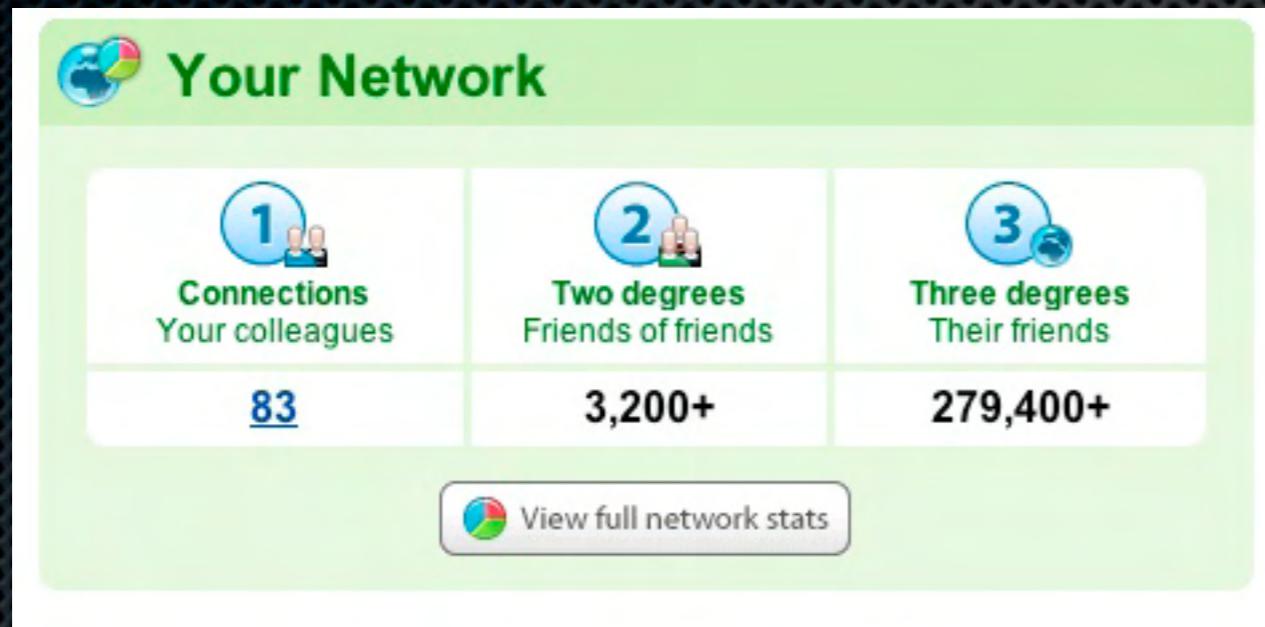
- Social networks



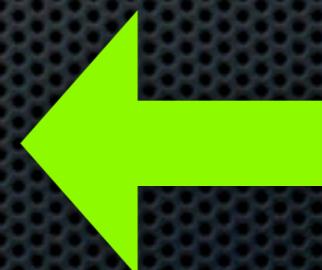
LinkedIn is an online network of more than 15 million experienced professionals from around the world, representing 150 industries.



Obtaining user info - New sources



Current Job
Past Jobs
Education
Job description
Etc...



Obtaining user info - New sources



You're looking for: **nasa**

The following number of people were found on XING matching your search for "nasa":

▶ Previous companies	179
▶ About me	168
▶ Company	145
▶ Haves	49

New search **Find**

Obtaining user info - theHarvester

```
Default (108,38)

libelibJulie Atwood
      Heather Landers
****  Pete Langlois
*The Megumi Nordby
*Coc Eric Dawson
*Edg Tobey Fitch
*cmc Solomon Eliashev
**** Conrad Klahn
      Jennifer Dockeray
      Neil Saunders
Usag Lance Hoffman
      Roy Riccomini
      Nick Hodge
      Ellen Pellens
      Bill Stevenson
      Matthew Formica
      Michael Agustin
      Dave Falkenburg
      Carsten Brinkschulte
      Stewart Hopkirk
Exam Steve Flinn
      Eric Shultz
      Phil Kirschner
      Noelle Gonzalez
libe Danese Cooper
      Ben DeVries
      Kathy Tafel
      Joe Interisano
      Mark Leabo
      Gregor Purdy
      Joe Jasinskas
      Nicholas Volodimer
      Kati Lechner
      Pete Petras
=====
Total results: 71
liberacion:/tools/edge/edgesec/theHarvester root# []
```

Obtaining Emails - theHarvester

```
Default (108,38)
liberacion:/tools/edge/edgesec/theHarvester root# python theHarvester.py -d "nasa.gov" -l 100 -b google
*****
*TheHarvester Ver. 1.4          *
*Coded by laramies              *
*Edge-Security Research         *
*cmartorella@edge-security.com  *
*****


Searching for nasa.gov in google :
=====

Total results: 12700000
Limit: 100
Searching results: 0

Accounts found:
=====

jim.arnold@msfc.nasa.gov
paul.meyer@msfc.nasa.gov
globus@nas.nasa.gov
help@sti.nasa.gov
earthweb@mail.nasa.gov
histinfo@hq.nasa.gov
E.Larko@nasa.gov
steven.m.graham.20gsfc.nasa.gov
starchild@heasarc.gsfc.nasa.gov
espenak@gsfc.nasa.gov
pierce@agnes.gsfc.nasa.gov
access@mail.arc.nasa.gov
=====

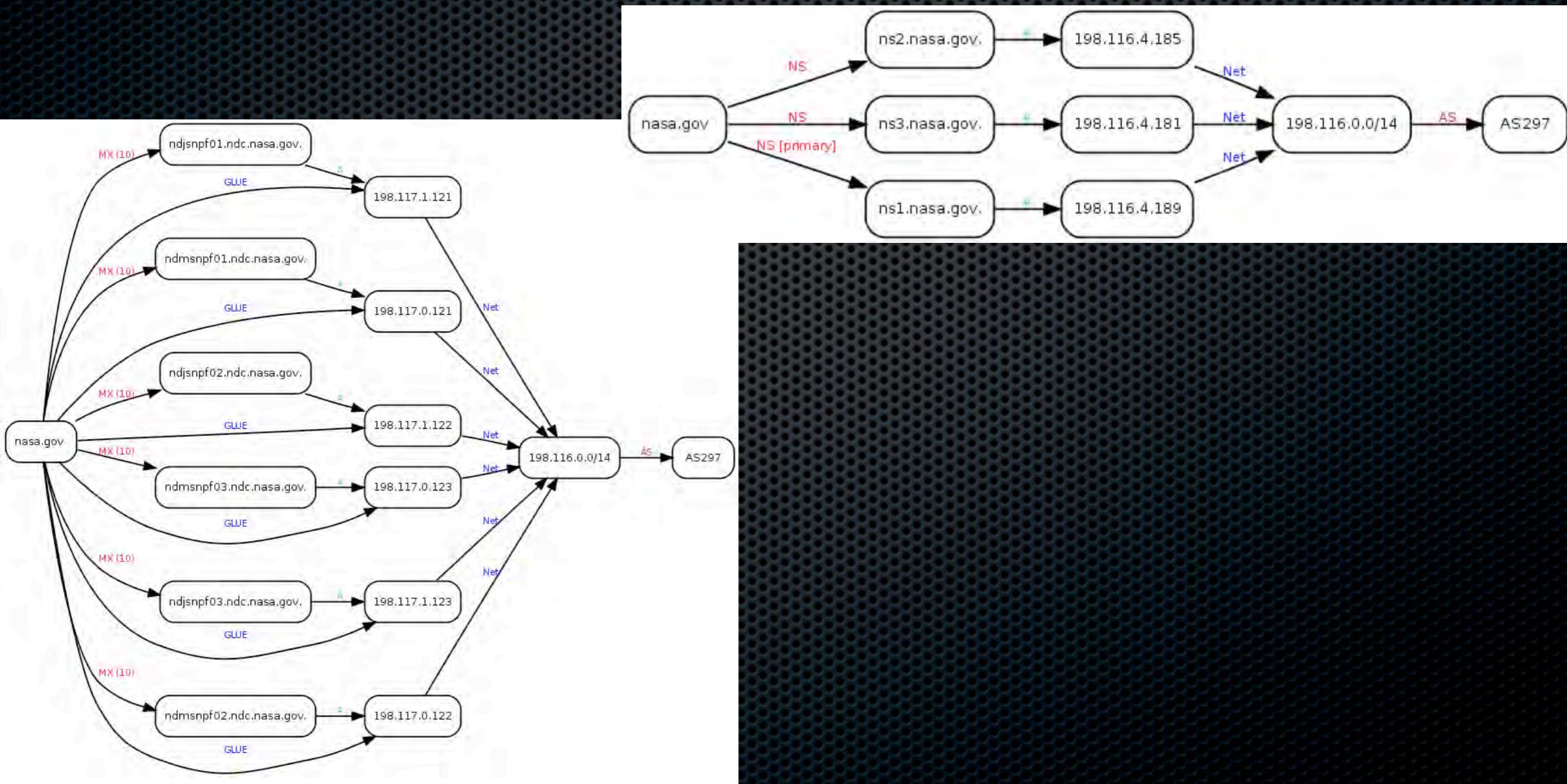
Total results: 12
liberacion:/tools/edge/edgesec/theHarvester root# []
```

Online tools



- ServerSniff.net:
 - NameServers reports (NS)
 - Autonomous Systems reports (AS)
 - Virtual hosts

Serversniff MX and NS Graphs



Obtaining more data - New sources

Metadata: is data about data.

Is used to facilitate the understanding, use and management of data.

Obtaining more data - New sources

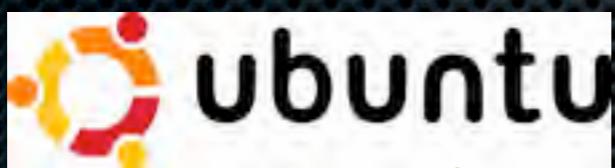
- Metadata

Provides basic information such as the author of a work, the date of creation, links to any related works, etc.

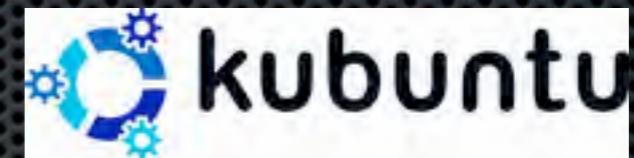
Metadata - Dublin Core (schema)

Content & about the Resource	Intellectual Property	Electronic or Physical manifestation
Title	Author or Creator	Date
Subject	Publisher	Type
Description	Contributor	Format
Language	Rights	Identifier
Relation		
Coverage		

Metadata - example



software - [Adobe ImageReady](#)
size - 1501x391
mimetype - image/png



logo-Kubuntu.png

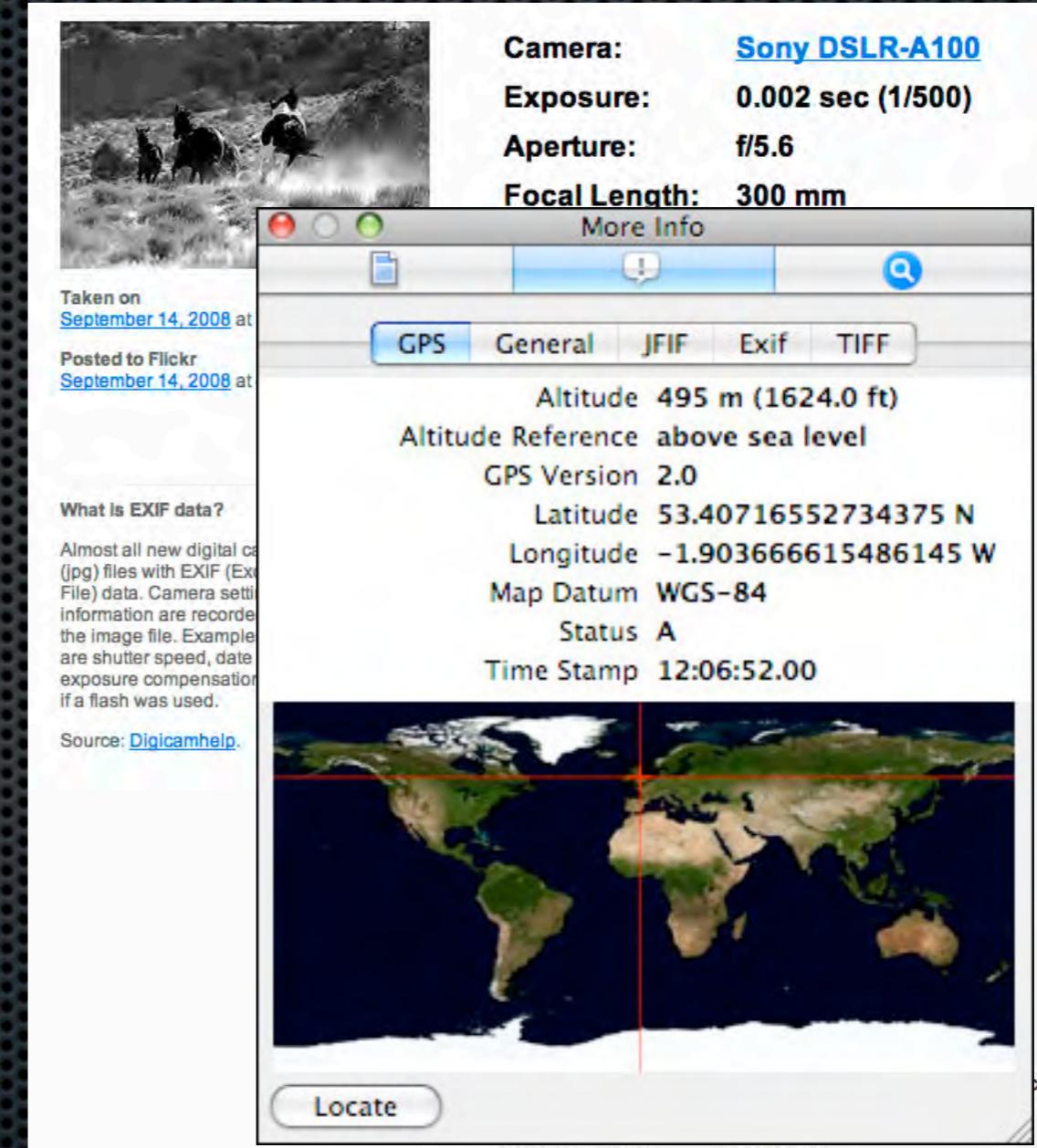


software - www.inkscape.org
size - 1501x379
mimetype - image/png

:/

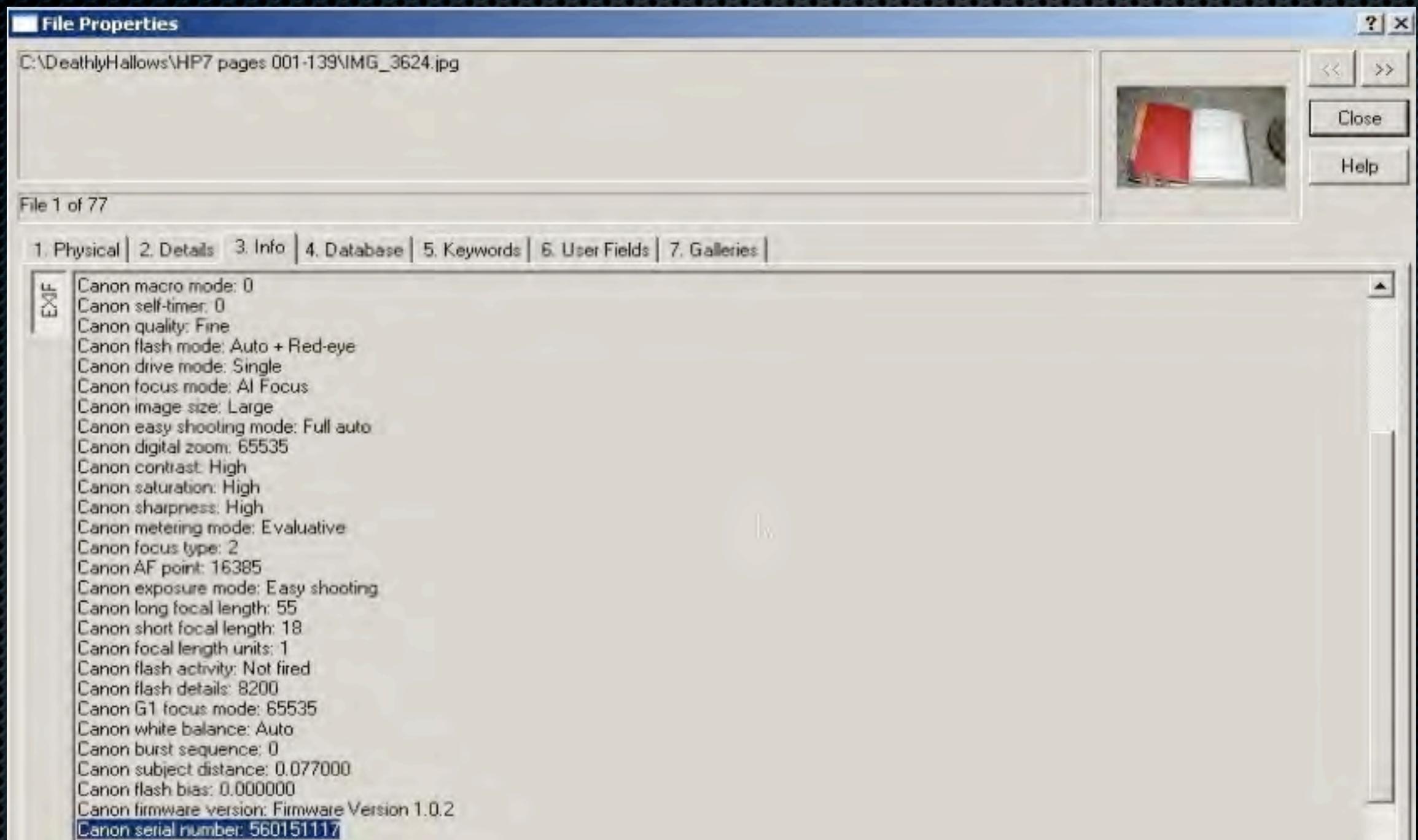
Metadata - Images

- EXIF Exchangeable Image File Format
 - GPS coordinates
 - Time
 - Camera type
 - Serial number
 - Sometimes unaltered original photo can be found in thumbnail
- Online exif viewer.



[Return to the Running Wild page.](#)

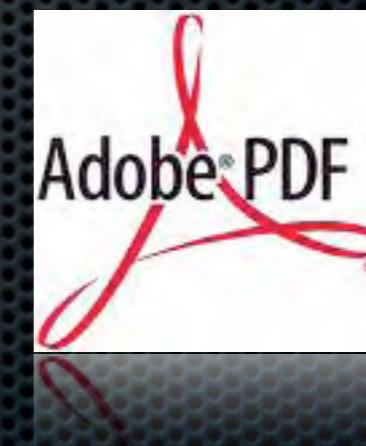
Metadata - EXIF- Harry Pwner



Deathly EXIF?

Metadata

- So where can we get interesting metadata?



Metadata

- Ok, I understand metadata... so what?

Metagoofil

- Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,etc) availables in the target/victim websites.

Metagoofil

User names

Workers
names

Server names

Paths

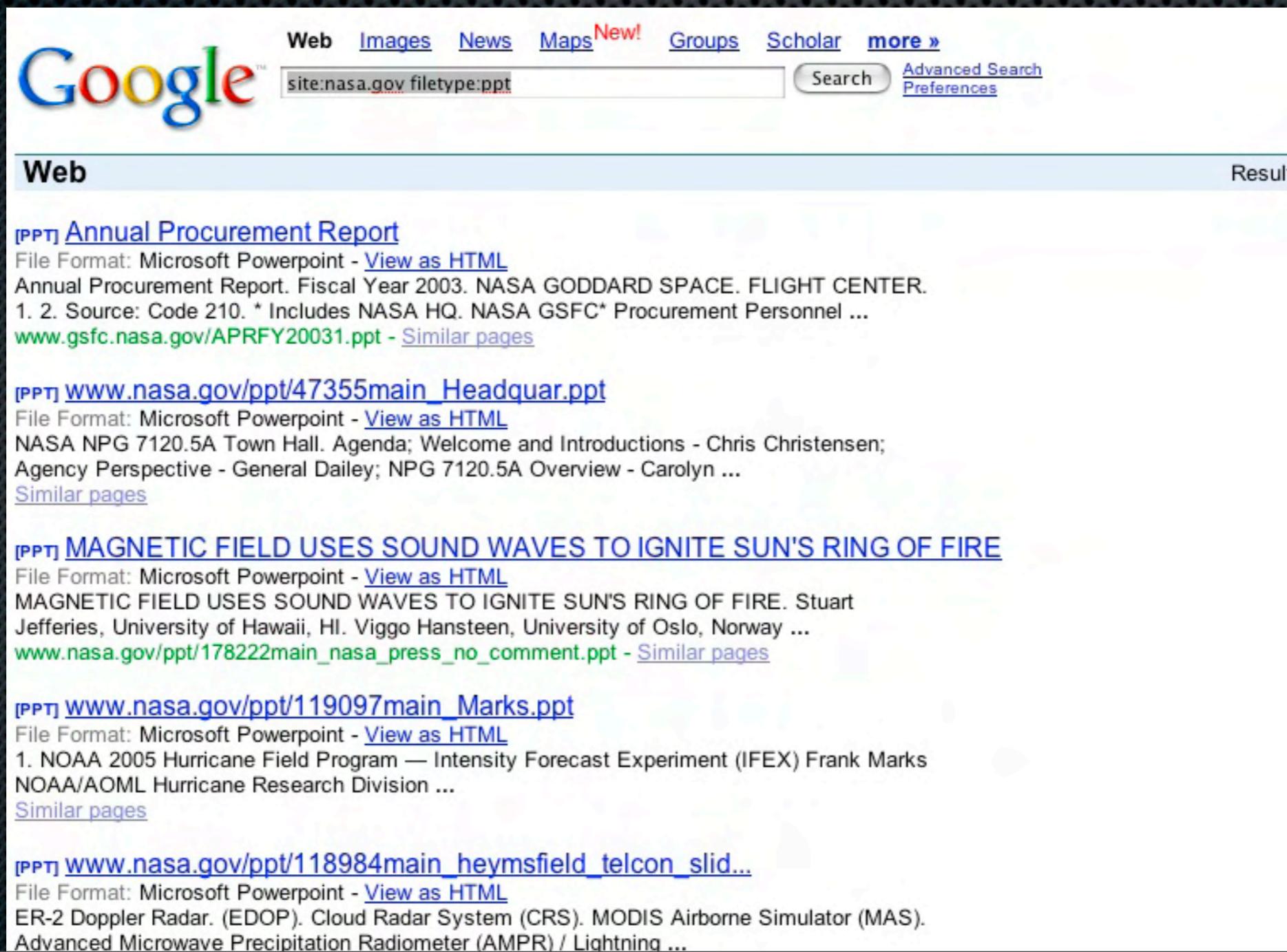
Software
versions + Date

Mac Address



Metagoofil

site:nasa.gov filetype:ppt



A screenshot of a Google search results page. The search query is "site:nasa.gov filetype:ppt". The results are filtered to show only web pages (Web tab selected). The first result is a Microsoft Powerpoint presentation titled "Annual Procurement Report" from NASA Goddard Space Flight Center, dated Fiscal Year 2003. The second result is a Microsoft Powerpoint presentation titled "www.nasa.gov/ppt/47355main_Headquar.ppt" from NASA NPG 7120.5A Town Hall. The third result is a Microsoft Powerpoint presentation titled "MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE" from Stuart Jefferies at the University of Hawaii. The fourth result is a Microsoft Powerpoint presentation titled "www.nasa.gov/ppt/119097main_Marks.ppt" from Frank Marks at NOAA/AOML Hurricane Research Division. The fifth result is a Microsoft Powerpoint presentation titled "www.nasa.gov/ppt/118984main_heymsfield_telcon_slid..." from the ER-2 Doppler Radar team.

Web Images News Maps New! Groups Scholar more »

site:nasa.gov filetype:ppt

Search Advanced Search Preferences

Web Results

[PPT] [Annual Procurement Report](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
Annual Procurement Report. Fiscal Year 2003. NASA GODDARD SPACE. FLIGHT CENTER.
1. 2. Source: Code 210. * Includes NASA HQ. NASA GSFC* Procurement Personnel ...
www.gsfc.nasa.gov/APRFY20031.ppt - [Similar pages](#)

[PPT] [www.nasa.gov/ppt/47355main_Headquar.ppt](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
NASA NPG 7120.5A Town Hall. Agenda; Welcome and Introductions - Chris Christensen;
Agency Perspective - General Dailey; NPG 7120.5A Overview - Carolyn ...
[Similar pages](#)

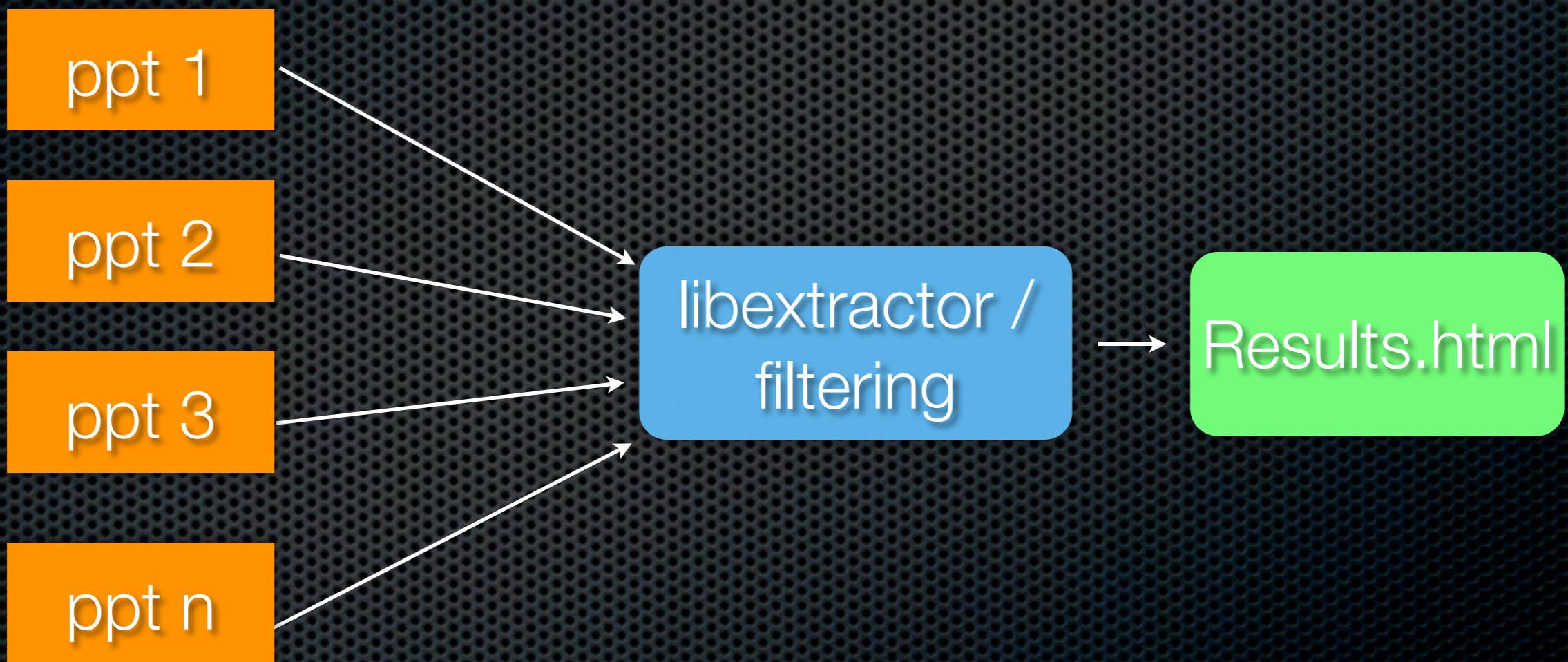
[PPT] [MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE. Stuart
Jefferies, University of Hawaii, HI. Viggo Hansteen, University of Oslo, Norway ...
www.nasa.gov/ppt/178222main_nasa_press_no_comment.ppt - [Similar pages](#)

[PPT] [www.nasa.gov/ppt/119097main_Marks.ppt](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
1. NOAA 2005 Hurricane Field Program — Intensity Forecast Experiment (IFEX) Frank Marks
NOAA/AOML Hurricane Research Division ...
[Similar pages](#)

[PPT] [www.nasa.gov/ppt/118984main_heymsfield_telcon_slid...](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
ER-2 Doppler Radar. (EDOP). Cloud Radar System (CRS). MODIS Airborne Simulator (MAS).
Advanced Microwave Precipitation Radiometer (AMPR) / Lightning ...

Metagoofil

Downloaded files



Metagoofil - results

http://lwsscience.gsfc.nasa.gov/Townsend_LWSWG.ppt

Local copy [Open](#)

Important metadata:

```
mimetype - application/vnd.ms-powerpoint
paragraph count - 181
last saved by - Lt
creation date - 2004-04-03T23:36:58Z
title - PowerPoint Presentation
word count - 974
creator - Lt
date - 2004-04-06T12:42:45Z
generator - Microsoft PowerPoint
```

http://saber.larc.nasa.gov/03SABER_non_LTE_algo_approach.ppt

Local copy, failed download :(

http://ldcm.nasa.gov/library/Analysis_L7ImageryPurchases_110501.ppt

Local copy [Open](#)

Important metadata:

```
mimetype - application/vnd.ms-powerpoint
paragraph count - 123
last saved by - RWIKER
template - C:\Documents and Settings\m10282\Application Data\Microsoft\Templates\mtek_briefing.pot
creation date - 2001-09-24T21:26:00Z
title - TitleHere
word count - 520
page count - 3
creator - Mitretek Systems
date - 2001-11-08T13:26:22Z
generator - Microsoft PowerPoint 4.0
```

<http://gsfctechnology.gsfc.nasa.gov/Code550procurement02012005.ppt>

Metagoofil - results

<http://weboflife.nasa.gov/1202.doc>

Local copy [Open](#)

Important metadata:

```
mimetype - application/msword
revision history - Revision #0: Author 'Philip T. Metzger' worked on ''
language - U.S. English
paragraph count - 2
line count - 10
last saved by - Philip T. Metzger
character count - 1258
template - Normal.dot
creation date - 2005-01-03T13:33:00Z
title - Penetrometer Testing of Transparent Granular Medium
word count - 220
page count - 1
creator - Masahiro Toiya
date - 2005-01-03T13:35:00Z
generator - Microsoft Word 10.0
```

<http://weboflife.nasa.gov/0704.doc>

Local copy [Open](#)

Important metadata:

```
mimetype - application/msword
revision history - Revision #0: Author 'Philip T. Metzger' worked on ''
language - U.S. English
paragraph count - 2
line count - 8
last saved by - Philip T. Metzger
character count - 1004
template - Normal.dot
creation date - 2005-01-03T17:01:00Z
title - Rapid Relaxation of a Granular Step
word count - 175
page count - 1
creator - akudrolli
date - 2005-01-03T17:01:00Z
generator - Microsoft Word 10.0
```

Metagoofil - results

<http://imdc.nasa.gov/IMDCPrework.xls>

Local copy [Open](#)

Important metadata:

```
mimetype - application/vnd.ms-excel
last saved by - fbuchananjones
creation date - 2000-08-11T18:35:34Z
title - Mission Requirements
creator - Corina Moore
date - 2005-10-24T15:51:06Z
generator - Microsoft Excel
```

http://www.nasa.gov/xls/151027main_121TVSked.xls

Local copy [Open](#)

Important metadata:

```
mimetype - application/vnd.ms-excel
last saved by - LMIT-ODIN
subject - STS-89 TV Schedule
creation date - 1997-02-06T21:58:03Z
title - 89TV Sked
creator - Eileen Walsh
date - 2006-06-23T18:38:27Z
generator - Microsoft Excel
```

http://www.nasa.gov/xls/163559main_LunarExplorationObjectives.xls

Local copy [Open](#)

Important metadata:

```
mimetype - application/vnd.ms-excel
last saved by - Audrey Schaffer
creation date - 2006-06-29T14:20:24Z
creator - LMIT ODIN
generator - Microsoft Excel
```

Metagoofil - results

http://www.nasa.gov/doc/47147main_pmsepstruc.doc

Local copy [Open](#)

Important metadata:

```
mimetype - application/msword
revision history - Revision #9: Author 'Jennifer Romeo' worked on 'romeo HD:Documents:Articles & News:Articles_PM
revision history - Revision #8: Author 'jwiater' worked on '\\RGINTS\Nasashared\PMSEP\PMSEP 6\Conference Structure
revision history - Revision #7: Author 'John Newcomb' worked on 'C:\My Documents\Scientific Man\Current Programs\'
revision history - Revision #6: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-9-02.c
revision history - Revision #5: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-9-02.c
revision history - Revision #4: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02.c
revision history - Revision #3: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02.c
revision history - Revision #2: Author 'Edutech User' worked on 'C:\WINDOWS\Temporary Internet Files\OLK4\PMSEP D
revision history - Revision #1: Author 'Edutech User' worked on 'C:\Documents and Settings\krobinson\Application
revision history - Revision #0: Author 'Edutech User' worked on 'C:\Documents and Settings\krobinson\Application
language - U.S. English
paragraph count - 13
line count - 55
last saved by - Jennifer Romeo
character count - 6717
template - Normal
creation date - 2002-08-12T14:24:00Z
title - CONFERENCE STRUCTURE
word count - 1178
page count - 5
creator - John Newcomb
date - 2002-08-12T14:24:00Z
generator - Microsoft Word 9.0
```

Metagoofil - results

Path Disclosure:

```
C:\Documents and Settings\baltner\Application Data\Microsoft\Word\  
C:\_ISEM\MyProjects\XMLCIO\projectPlan\  
C:\Documents and Settings\rbenedic\My Documents\XML\NASA XML\XML Business Case\Final Business Case\  
    Normal\  
C:\WINNT\Personal\  
\  
U:\users\smarucci\A1\Writing\Internet\HOMEPAGE\cs\  
U:\code_hk\Competitive Sourcing\Ten Year Look Back\  
C:\Documents and Settings\jlecren\Application Data\Microsoft\Word\  
C:\My Documents\2Ldp\Website\2005 Web Site Update\Reports\  
C:\My Documents\2Ldp\2005-06\1Orientation\1Participants\2Orientation Binder\Section D Reports\  
C:\My Documents\2Ldp\2005-06\1Orientation\1Participants\2Orientation Binder\Section D\  
C:\My Documents\2Ldp\2004-05\07Orientation\Participants\2Orientation Binder\Section D\  
C:\My Documents\2Ldp\Website\2004 Update\11Reports\  
C:\Documents and Settings\rbenedic\Application Data\Microsoft\Word\  
C:\Documents and Settings\rbenedic\My Documents\XML\NASA XML\NASA XML Project Plan\NASA XML Project Plan Revision  
\RGIANTS\Nasashared\PMSEP\PMSEP 6\Structure\  
C:\My Documents\Scientific Man\Current Programs\EduTech Work\PMSEP Folder\Structure\Present Structure\  
C:\My Documents\  
C:\WINDOWS\Temporary Internet Files\OLK4\  
C:\Documents and Settings\krobinson\Application Data\Microsoft\Word\  
U:\users\kbayer\IOY03\  
C:\Documents and Settings\u4ri9mah\My Documents\Rocket Blast\KSC Meeting\  
C:\Documents and Settings\u4ri9mah\Application Data\Microsoft\Word\  
C:\Documents and Settings\pcurto\Desktop\  
V:\  
A:\  
C:\Documents and Settings\akennedy\My Documents\Data\attach\  
U:\users\kbayer\DATA\Word\  
Macintosh HD:Users:mls:Documents1:Documents:student travel:Hemispheresapp\  
Macintosh HD:Documents:student travel:Hemispheresapp\  
Macintosh HD:Documents:student travel:astrobiology workshop:ABstudentapp\  
Macintosh HD:Users:mls:Desktop:astrobiology workshop:ABstudentapp\  
C:\Documents and Settings\lucero james\Desktop\  
C:\Documents and Settings\cordova cecilia\Desktop\PDP\FY03PDPDescrip\  
C:\Documents and Settings\cordova cecilia\Desktop\PDP\  
C:\CECILIAS0998\Word0998\PDPAug99\  
Gwen Young:Desktop Folder:Gwen\  
    C:\Program Files\Microsoft Office\Templates\Presentation Designs\  
D:\Microsoft Office\Templates\Presentation Designs\  
C:\Program Files\Office2K\Templates\Presentation Designs\  
Macintosh HD:Users:pmhughes:Documents:PH'sDocs:** Peter's Data* ::* GSFC R&TD  *:FY07 R&TD Planning:FY07 IntegInvE  
C:\WINDOWS\Desktop\
```

Metagoofill results

RÄYÄLÄÄ9RÄ\8\\nÄ“TUÄ³\(\Ä¹
KÄ! " ¶ÄŠÄ“Ä©Äl Ä±Ä®ÄlÄ
Ä“Ä±ÄŽRÄÄ„+TÄ“Ä“WE&[
Ä“-Ä>f\)HÄtnj "Ä³S
Ä·IÄrÄi Ä·- Ä·\(\Ä±-ÄfÄkÄ-
Ä·ÄpÄ, Ä·-ÄpÄ, Ä·-Äo Ä·-Ä-
Ä·-Ä] 3Ä „ n8Ä LÄSHÄk- ;
Ä“Ä±ÄXÄ Ä‘vÄ| ^!Ä“ÄkÄ+ÄzÄ
JYfSAZ UÄ“Ä‘ÄÄ“y
Ä·Ä“8Ä“YÄ‘!* Ä©vÄ“ÄfÄ“'ÄzÄmVÄkÄ«FuÄ“Ä‘Ä‘7Ä-Ä+|Ä
ÄÄ‘ÄžÄt> JEzÄ—6ÄkÄzÄYÄpÄ~ÄI#ÄZÄ, Ä¢TN
Ä“Ä-Ä·DÄ·ÄthÄÄ«Ä·ÄzÄ³ÄihC8UÄ¶SÄ‘7G
+Ä“ÄiÄm\)Ä+Ä+ÄkÄ°ÄsÄ“ÄD'!Ä“
Ä‘\n1Q\rÄiÄ,7DBÄ“:g\Ä~
VÄtÄ‘Ä·RÄäÄž<-Ä-Ä®->10K}ÄeÄÄ-KÄ...Ä¶ÄŠY->|
baltner
rbenedic
mdale
Chris Williams
pcurto
Philip T. Metzger
Nand Lal
Susan Hoban
PAC
Software Management Facility
ganesh
susie marucci
jlecren
Ron Lentz
M Dale
odomjd
Robert Benedict
WALTER KIT
Jennifer Romeo
jwiater
John Newcomb
Edutech User
SAIC-ODIN-NASA HQ
BEAVER
Tanya
ardonem
rmirelso
MacP49 LASP
Lab 157
Robert Sullivan
Charles Campbell

Jerome Johnson
Charles Collins
Christopher Brunner
Barry Coutermarsh
NETL User
Richard Williams
sture
u4ri9mah
Schiffer
Peter Schiffer
Richard Schultz
ERDC User
U4GM9DLS
Duan Z. Zhang
Sarah Martinez
ODIN Seat User
Scott B. Jones
Markus Tuller
R. P. Behringer
Leonardo F. Silbert

Metagoofil & Linkedin results

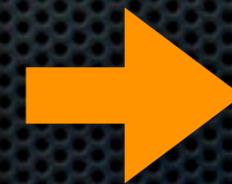
- Now we have a lot of information, what can i do?
 - User profiling
 - Spear Phishing / Social Engineering
 - Client side attacks

Using results

- User profiling
- Dictionary creation John Doe



john.doe
jdoe
j.doe
johndoe
johnd
john.d
jd
doe
john



ATTACK!

Metadata - The Revisionist

- Tool developed by Michal Zalewski, this tool will extract comments and “Track changes” from Word documents.

Finally, Microsoft is an enduring company ~~that's not going out of business (unlike many Linux vendors)~~. We're committed to providing IT flexibility and growth options to our customers so they can continue to rely on their Microsoft-based IT infrastructure to quickly respond to a competitive marketplace.

<http://download.microsoft.com/download/3/4/9/349c2166-4d53-43f6-b1fd-970090e23216/PARTNER/MSFreeShop.doc>

Target information:

- Email account
- Google Finance, Reuters
- pipl.com 
- Usercheck.com

Google Finance & Reuters

Officers and directors

Kenneth D. Lewis >	Chairman of the Board, President, Chief Executive Officer
Joe L. Price >	Chief Financial Officer
Barbara J. Desoer >	President of the New Bank of America Mortgage, Home Equity & Insurance Services Business
Liam E. McGee >	President - Global Consumer and Small Business Banking
Brian T. Moynihan >	President - Global Corporate and Investment Banking
Keith T. Banks >	President - Global Wealth and Investment Management
Bruce L. Hammonds >	President - Global Card Services
Craig R. Rosato >	Chief Accounting Officer
J. Steele Alphin >	Chief Administrative Officer
Amy Woods Brinkley >	Global Risk Executive

[Full list on Reuters »](#)

Summary	Biographies	Basic Compensation	Options Compensation
Name	Age	Since	Current Position ▾
Desoer, Barbara	55	2008	President of the New Bank of America Mortgage, Home Equity & Insurance Services Business
Banks, Keith	52	2007	President - Global Wealth and Investment Management
Moynihan, Brian	48	2007	President - Global Corporate and Investment Banking
McGee, Liam	53	2004	President - Global Consumer and Small Business Banking
Hammonds, Bruce	—	2008	President - Global Card Services
Sloan, O. Temple	69	2006	Lead Director
Brinkley, Amy	52	2008	Global Risk Executive
Massey, Walter	70	1998	Director
Spangler, Meredith	70	1988	Director
Ward, Jacquelyn	70	1994	Director
Mitchell, Patricia	65	2001	Director
Gifford, Charles	65	2005	Director
Barnet, William	65	2004	Director
Collins, John	61	2004	Director
Countryman, Gary	68	2004	Director
May, Thomas	60	2004	Director
Ryan, Thomas	55	2004	Director
Franks, Tommy	62	2005	Director
Bramble, Frank	59	2006	Director
Tillman, Robert	64	2005	Director
Lozano, Monica	51	—	Director

Searching for a target

pipl

christian	Martorella		ES	Search	Clear
First Name	Last Name	City	State	Country	

Christian Martorella, Spain

Professional & Business

 [Christian Martorella, Manager, Computer & Network Security, ES...
Professional Profile & Networking - LinkedIn](#) www.linkedin.com

Results for Christian Martorella without Spain

Personal Profiles

 [Christian Martorella...
Customer Profile - Amazon.com](#) www.amazon.com - Deep Web

 [Christian Martorella...
Personal Web Profile - Facebook](#) www.facebook.com

 [Christian Martorella...
Personal Web Profile - Facebook](#) www.facebook.com

Publications

 [Laramies Corner: Memoryze - Memory forensic tool. 11 Nov 2008 by Christian...
Blog Posts - Google Blog Search](#) laramies.blogspot.com

 [Laramies Corner, - http://laramies.blogspot.com/...
Blog Posts - Google Blog Search](#) blogsearch.google.com

Email Address

 ... researched by: - Alberto Moro <amoro@s21sec.com> S21Sec With thanks to: -
[Christian Martorella <cmartorella@s21sec.com> S21Sec \[REFERENCES \] * Timbuktu ...
S21Sec Advisory ...](#) www.s21sec.com

 Advanced web application defense with Modsecurity. Daniel Fernandez Bleda.
[dfernandez@isecauditors.com. Christian Martorella. cmartorella@isecauditors.com.](#) wiki.whatthehack.org
Advanced Web Application Defense with ModSecurity

Web Pages

web and image results enhanced by 

 [Christian Martorella. Gender: Male; Industry: Technology; Occupation: Security
Engineer; Location: Barcelona : Catalunya : Spain ...
Blogger: User Profile: Christian Martorella](#) www.blogger.com

 [Christian Martorella. From What The Wiki?! Advanced Web Application Security Defense
with ModSecurity • Click for more details... Click for more details.
Christian Martorella - What The Wiki?!](#) wiki.whatthehack.org

 [OISSG - Open Information Systems Security Group website.
Christian Martorella. General Information for the Security G...](#) www.oissg.org

Usercheck.com

USERNAME: laramies

 12seconds - available	 ILikeTotallyLoveIt - available	 Steam - available
 Behance - available	 Imageshack - available	 Stumbleupon - available
 Blogger - taken	 Isfingawesome - available	 Technorati - available
 Brightkite - available	 Jaiku - available	 Tinyurl - available
 Colourlovers - available	 Koornk - available	 Tipd - available
 Corkd - available	 Kwippy - available	 Tipjoy - available
 Dailymotion - available	 Lastfm - taken	 Tumblr - available
 Delicious - taken	 Linkedin - available	 Twitter - available
 Digg - available	 Livejournal - taken	 Typepad - available
 Diigo - taken	 Magnolia - available	 Uservoice - available
 Disqus - available	 Meemi - available	 Ustream - available
 Ebay - taken	 Mixx - available	 Vimeo - taken
 Etsy - taken	 Multiply - available	 Virb - available
 Favtape - available	 Myspace - taken	 Visualizeus - available
 Fffound - available	 Odeo - available	 Vox - available
 Flickr - taken	 Pandora - available	 Wakoopa - available
 Friendfeed - available	 Picasa - taken	 Wordpress - available
 Funnyordie - available	 Plurk - available	 Xing - available
 Gmail - taken	 Posterous - available	 Yahoo - taken
 Hellobox - available	 Pownce - available	 Yotify - available
 Hexday - available	 Rejaw - available	 Youtube - taken

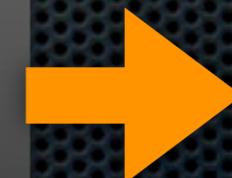
Using results

- Password profiling

Dictionary creation: words from the different user sites



magic
serra angel
necropotence
Shivan dragon
elf
brainstorm
...
...



**Brute force
ATTACK**

There are more ways to get info



33663
Q1 08
7.31.08
Caroline Flint - Speaking Note
State of Housing market

- Colleagues will know this present.
- Leading house price index falls for the first time in recent years. Given present trends, they will clearly show sizeable falls in prices later this year – at best down 5-10% year-on-year.
- House building is also stalling. New starts are already down 10% compared to a year ago. Housebuilders are predicting further falls. Having seen net additions reach roughly 200,000 in each of the last two years, the figure for 2008-09 is almost certain to be well down on that.
- Repossessions are also rising, although we need to remember that the 2007 figure was still only around a third of that in 1991.
- Underlying demand for housing remains high and the fundamentals of the economy are sound. But the market is being affected by the global credit crunch, which is making it difficult for many who would like to buy to do so.
- We can't know how bad it will get. But we need to plan now to put in place effective measures against the risk that it does get worse and to prepare for the up-turn.
- We are continuing to monitor the situation, and take appropriate action.
- The Chancellor and I met some of the largest mortgage lenders recently to continue discussions on what more the Government and the industry could be doing. I have subsequently met a number of the smaller lenders.
- We are playing our part to get the market moving with the Bank of England's £50 billion liquidity scheme. We have also put in place new measures to ensure the small minority of buyers facing repossession receive the support and advice they need. And I will tomorrow announce a package of measures to assist first time buyers.

But it is vital that we show that at this time of uncertainty we show that we are on people's side:

Facebook

facebook

Phone in sick and treat himself to a day in bed.



Kyle Doyle
is not going to work. f [REDACTED] it
Updated on Thursday

Networks:	Au
Sex:	Ma
Interested In:	W
Birthday:	Ja
Hometown:	Sy
Political Views:	Lib
Religious Views:	Ag

Kyle Doyle's Facebook profile makes it quite obvious he was not off work for a 'valid medical reason'

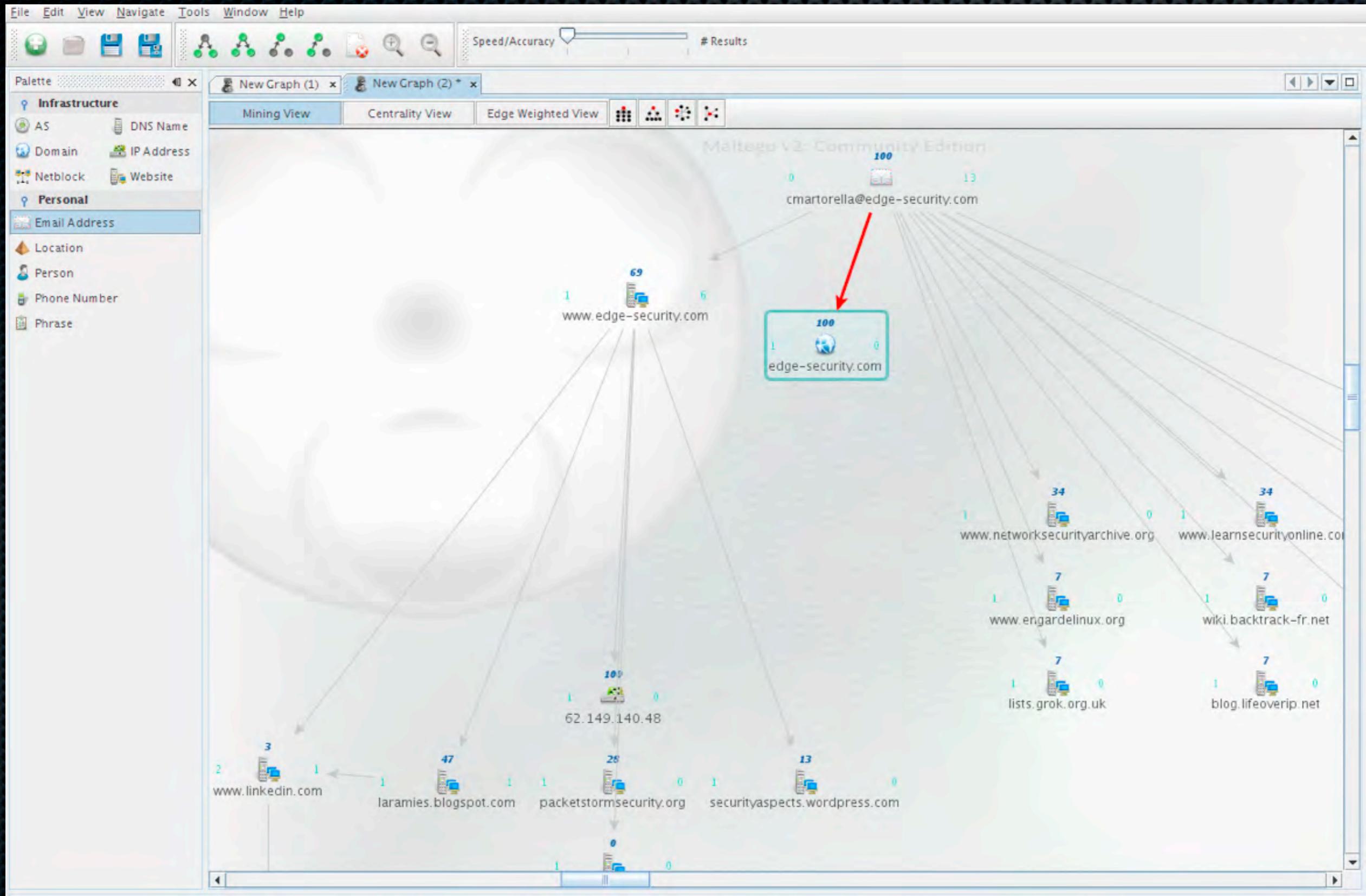
All together - Maltego



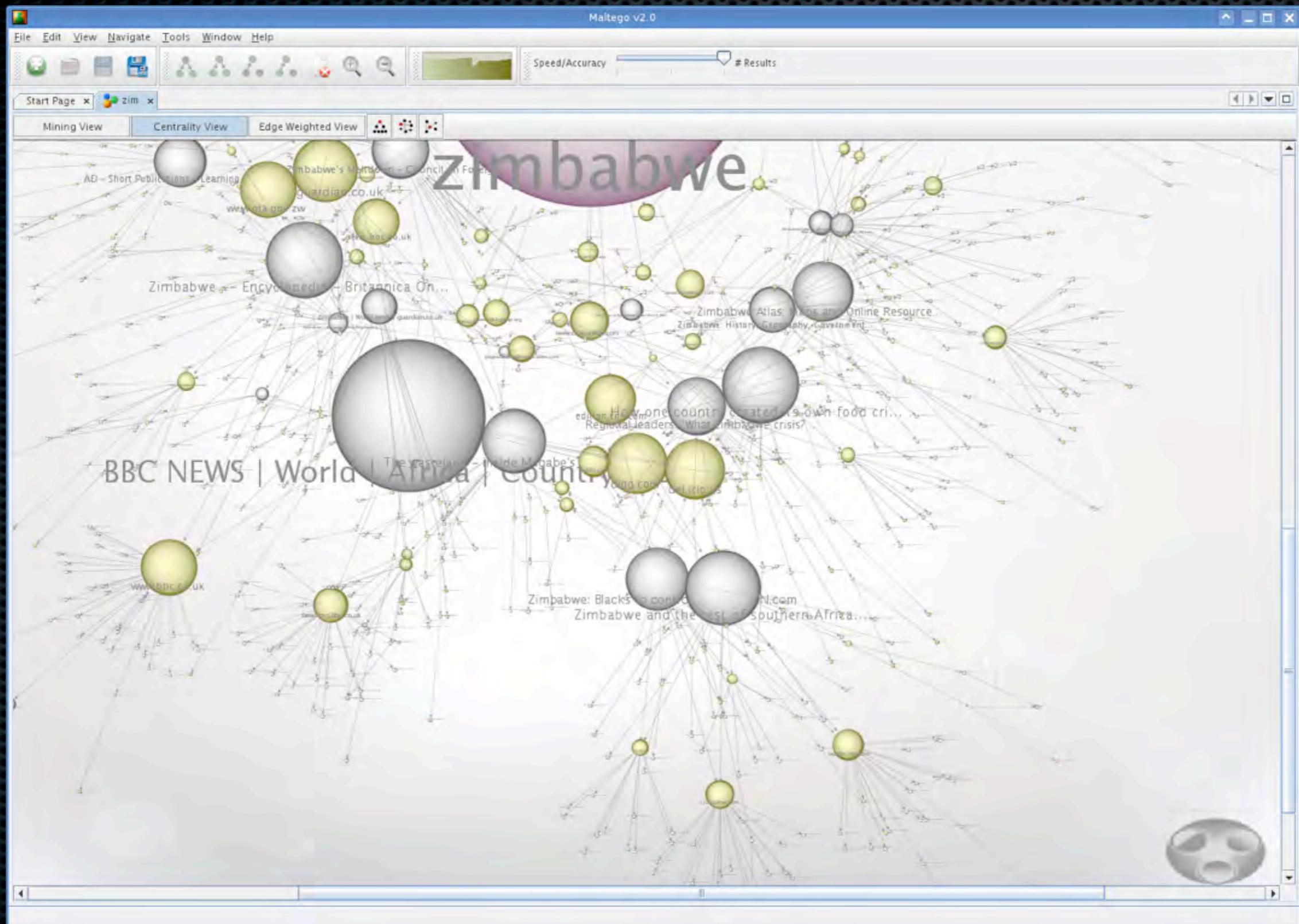
Maltego is “the only” professional Information Gathering tool.

“Information is power
Information is Maltego”

Maltego



Maltego



Conclusions

- Clean your files before distribution
- Web applications should clean files on upload (if it's not needed)
- Web applications should try to represent the information in a non parseable way :/
- Be careful what you post/send

References

- www.edge-security.com
- blog.s21sec.com
- www.s21sec.com
- carnal0wnage.blogspot.com
- www.gnunet.org/libextractor
- lcamtuf.coredump.cx/strikeout/
- www.paterva.com





Tomorrow's Digital Security, Today

Thank you for coming

cmartorella@s21sec.com

cmartorella@edge-security.com