

# A fresh new look into Information Gathering V2



**Christian Martorella**  
FIST Conference March 2009

 **S21sec**  
Tomorrow's Digital Security, Today



# Who am i ?

## Christian Martorella

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



# 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.”



# Types of I.G

**Passive**

**Active**



# I.G what for?

- ✦ **Infraestructure:**

Information for discovering new targets, to get a description of the hosts (NS,MX, AS,etc), shared resources, applications, software, etc.

- ✦ **People and organizations:**

For performing brute force attacks on available services, Spear phishing, social engineering, investigations, analysis, background checks, information leaks, client side exploits



How can we obtain this kind  
of info?



# Obtaining info - Classic way

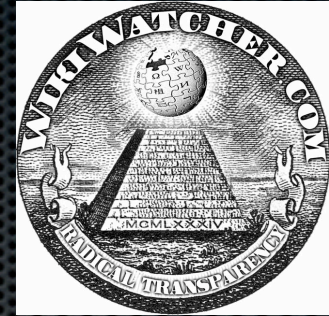
- ✦ Zone Transfer (active)
- ✦ Whois (passive)
- ✦ Reverse Lookup (active)
- ✦ BruteForce (active++)
- ✦ Mail headers (active)
- ✦ smtp (active++)
- ✦ Search engines
- ✦ PGP Key Servers
- ✦ [serversniff.net](http://serversniff.net)



New sources for I.G ...



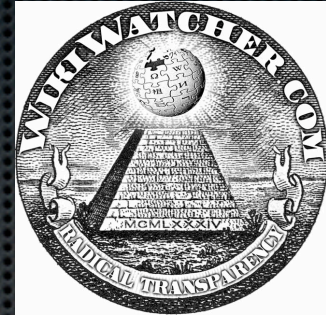
# WikiScanner



- ✦ When you edit the wikipedia:
  - ✦ You can edit leaving your username
  - ✦ You can edit anonymous using your IP address



# 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*

<input type="checkbox"/>	IP Range	Name	Domain	Location	EN edits	DE edits	JA Edits
<input type="checkbox"/>	<a href="#">171.159.129.0-160.231.255</a>	<a href="#">Bank Of America</a>	<a href="#">pacbell.net</a> <small>[web]</small>	<a href="#">Concord, California</a> , United States	1396	1	0
<input type="checkbox"/>	<a href="#">171.161.160.0-255</a>	<a href="#">Bank Of America</a>	<a href="#">pacbell.net</a> <small>[web]</small>	<a href="#">Dallas, Texas</a> , United States	990	8	0
<input type="checkbox"/>	<a href="#">171.159.64.0-255</a>	<a href="#">Bank Of America</a>	<a href="#">pacbell.net</a> <small>[web]</small>	<a href="#">Walnut Creek, California</a> , United States	827	1	0
<input type="checkbox"/>	<a href="#">171.161.224.0-255</a>	<a href="#">Bank Of America</a>	<a href="#">bankofamerica.com</a> <small>[web]</small>	<a href="#">Charlotte, North Carolina</a> , United States	605	0	0
<input type="checkbox"/>	<a href="#">171.191.65.0-196.96.255</a>	<a href="#">Bank Of America</a>	<a href="#">pacbell.net</a> <small>[web]</small>	<a href="#">Concord, California</a> , United States	223	0	0
<input type="checkbox"/>	<a href="#">171.161.96.0-255</a>	<a href="#">Bank Of America</a>	<a href="#">bankofamerica.com</a> <small>[web]</small>	<a href="#">Pasadena, California</a> , United States	199	0	0
<input type="checkbox"/>	<a href="#">171.158.6.0-159.63.255</a>	<a href="#">Bank Of America</a>	<a href="#">davita.com</a> <small>[web]</small>	<a href="#">Concord, California</a> , United States	103	38	0
<input type="checkbox"/>	<a href="#">171.160.233.0-161.95.255</a>	<a href="#">Bank Of America</a>	<a href="#">pacbell.net</a> <small>[web]</small>	<a href="#">Concord, California</a> , United States	82	0	0
<input type="checkbox"/>	<a href="#">171.159.128.0-255</a>	<a href="#">Bank Of America</a>	<a href="#">bankofamerica.com</a> <small>[web]</small>	<a href="#">Chicago, Illinois</a> , United States	22	0	0
<input type="checkbox"/>	<a href="#">63.148.5.0-63</a>	<a href="#">Woori America Bank</a>	<a href="#">qwest.net</a> <small>[web]</small>	<a href="#">Flushing, New York</a> , United States	19	0	0
<input type="checkbox"/>	<a href="#">206.229.105.0-63</a>	<a href="#">First National Bank Of America</a>	-	<a href="#">East Lansing, Michigan</a> , United States	14	0	0
<input type="checkbox"/>	<a href="#">69.208.102.112-119</a>	<a href="#">Mid America Bank</a>	-	<a href="#">Chicago, Illinois</a> , 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
<a href="#">171.159.128.10</a>	1974 in film <a href="#">[cur]</a>	<a href="#">5080980</a>	<i>/* Other Movies Released */</i>	2004-07-14 13:33:06
<a href="#">171.159.128.10</a>	Bosch reaction <a href="#">[cur]</a>	<a href="#">4928021</a>		2004-06-25 14:10:03
<a href="#">171.159.128.10</a>	Evangelical Lutheran Synod <a href="#">[cur]</a>	<a href="#">13907709</a>	<i>/* History */</i>	2005-03-30 16:13:13
<a href="#">171.159.128.10</a>	Fencing <a href="#">[cur]</a>	<a href="#">4821554</a>	<i>/* Notable modern fencers and fencing masters */</i>	2004-07-23 19:18:12
<a href="#">171.159.128.10</a>	IBM Rational ClearCase <a href="#">[cur]</a>	<a href="#">4260457</a>		2004-06-24 17:54:29
<a href="#">171.159.128.10</a>	Lutheranism <a href="#">[cur]</a>	<a href="#">11739455</a>	<i>/* Denomination organization */</i>	2005-03-30 15:57:53
<a href="#">171.159.128.10</a>	MediaWiki talk:Recentchangestext <a href="#">[cur]</a>	<a href="#">4021222</a>	<i>/* Requested Articles */</i>	2004-06-10 18:13:44
<a href="#">171.159.128.10</a>	MOD (file format) <a href="#">[cur]</a>	<a href="#">7042652</a>	<i>/* Software */</i>	2004-09-21 15:54:12
<a href="#">171.159.128.10</a>	Prior art <a href="#">[cur]</a>	<a href="#">5147269</a>	<i>/* First-to-file systems */</i>	2004-08-11 18:38:52
<a href="#">171.159.128.10</a>	Terraforming <a href="#">[cur]</a>	<a href="#">4262808</a>		2004-06-24 19:46:46
<a href="#">171.159.128.10</a>	Terraforming <a href="#">[cur]</a>	<a href="#">4263486</a>	<i>/* Converting atmosphere */</i>	2004-06-24 19:54:23
<a href="#">171.159.128.10</a>	Terraforming <a href="#">[cur]</a>	<a href="#">4264445</a>	<i>/* In fiction */</i>	2004-06-24 21:25:47
<a href="#">171.159.128.10</a>	Terraforming <a href="#">[cur]</a>	<a href="#">4264707</a>	<i>/* History */</i>	2004-06-24 21:45:24
<a href="#">171.159.128.10</a>	Terraforming <a href="#">[cur]</a>	<a href="#">4264749</a>	<i>/* Ethical issues */</i>	2004-06-24 21:50:27
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810524</a>		2004-07-23 22:17:46
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810537</a>		2004-07-23 22:18:46
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810548</a>		2004-07-23 22:19:58
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810611</a>		2004-07-23 22:20:51
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810820</a>		2004-07-23 22:25:38
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810835</a>		2004-07-23 22:35:51
<a href="#">171.159.128.10</a>	Vladimir Nazlymov <a href="#">[cur]</a>	<a href="#">4810984</a>		2004-07-23 22:36:34
<a href="#">171.159.128.10</a>	Wikipedia:Introduction <a href="#">[cur]</a>	<a href="#">13800404</a>		2005-05-16 20:29:48



# Poor Man Check User

- ✦ Provide an ip for a wikipedia username

## Poor Man's Checkuser v1.2

by [Virgil](#) Griffith  
virgil at caltech dot edu

Searching 17864 unique IPs across 14166 unique usernames.

*This is not a tool that provides answers, it provides clues that require subsequent verification.* Connections with a yellow background are frequently inaccurate. Connections with a 🟡 are especially suspect.

### Search by username

Username

### Browse all users

[ [only greens](#) ] [ [greens+yellows](#) ]



# Obtaining user info - New sources

- Social Networks (passive)
- Metadata (passive)



# Obtaining user info - New sources

- Social networks

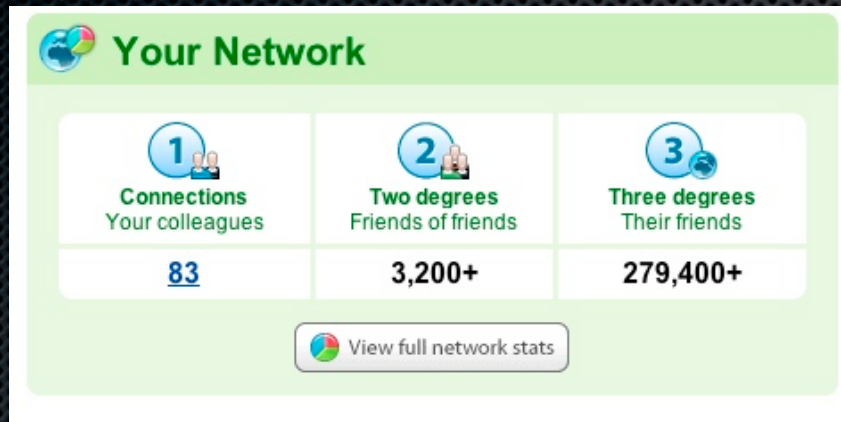


LinkedIn is an online network of more than 15 million experienced professionals from around the world, representing 150 industries.

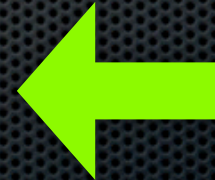




# Obtaining **user info** - New sources




Current Job  
Pasts 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":

▶	<b>Previous companies</b>	<b>179</b>
▶	<b>About me</b>	<b>168</b>
▶	<b>Company</b>	<b>145</b>
▶	<b>Haves</b>	<b>49</b>

**New search**  **Find**



# Obtaining **user names** from a company



```
Default (108,38)
Julie Atwood
Heather Landers
Pete Langlois
Megumi Nordby
Eric Dawson
Tabey Fitch
Solomon Eljashev
Conrad Klahn
Jennifer Dockeray
Neil Saunders
Lance Hoffman
Roy Riccomini
Nick Hodge
Ellen Pellens
Bill Stevenson
Matthew Formica
Michael Agustin
Dave Falkenburg
Carsten Brinkschulte
Stewart Hopkirk
Steve Flinn
Eric Shultz
Phil Kirschner
Noelle Gonzalez
Danese Cooper
Ben DeVries
Kathy Tafel
Joe Interisano
Mark Leabo
Gregor Purdy
Joe Jasinskis
Nicholas Volodimer
Kati Lechner
Pete Petras
=====
Total results: 71
liberacion:/tools/edge/edgesec/theHarvester root#
```



# Obtaining Emails from a company

```
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.2@gsfc.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#
```



# Linkedin pwn



**splunk**>

"Splunk provides a level of global cyber threat environment awareness that has never been possible before."

- John Topp,  
Technical Director,  
Major Government Agency

Free Download

**FAIL**

Industry Information Technology and Services

connections 50 connections



# 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)

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



# Metadata example

Las reglas del Dinero.doc Properties

General Summary Statistics Contents Custom

Title: Me and my metadata

Subject:

Author: Christian Martorella

Manager:

Company:

Category:

Keywords: Metadata, security, information gathering

Comments: This is my metadata

Hyperlink base: <http://www.edge-security.com>

Template: Normal.dotm

☒ Save preview picture with this document

Cancel OK

Las reglas del Dinero.doc Properties

General Summary Statistics Contents Custom

Created: Tuesday, August 7, 2007 8:31 PM

Modified: Tuesday, August 7, 2007 8:35 PM

Printed:

Last saved by: Christian Martorella

Revision number: 1

Total editing time: 4 Minutes

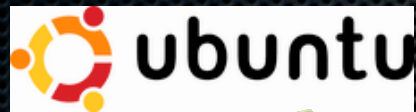
Statistics:

Statistic name	Value
Characters (with spaces):	495
Characters:	395
Words:	119
Lines:	27
Paragraphs:	21
Pages:	1

Cancel OK



# Metadata - example



software - **Adobe ImageReady**  
size - 1501x391  
mimetype - image/png



logo-Kubuntu.png



software - [www.inkscape.org](http://www.inkscape.org)  
size - 1501x379  
mimetype - image/png

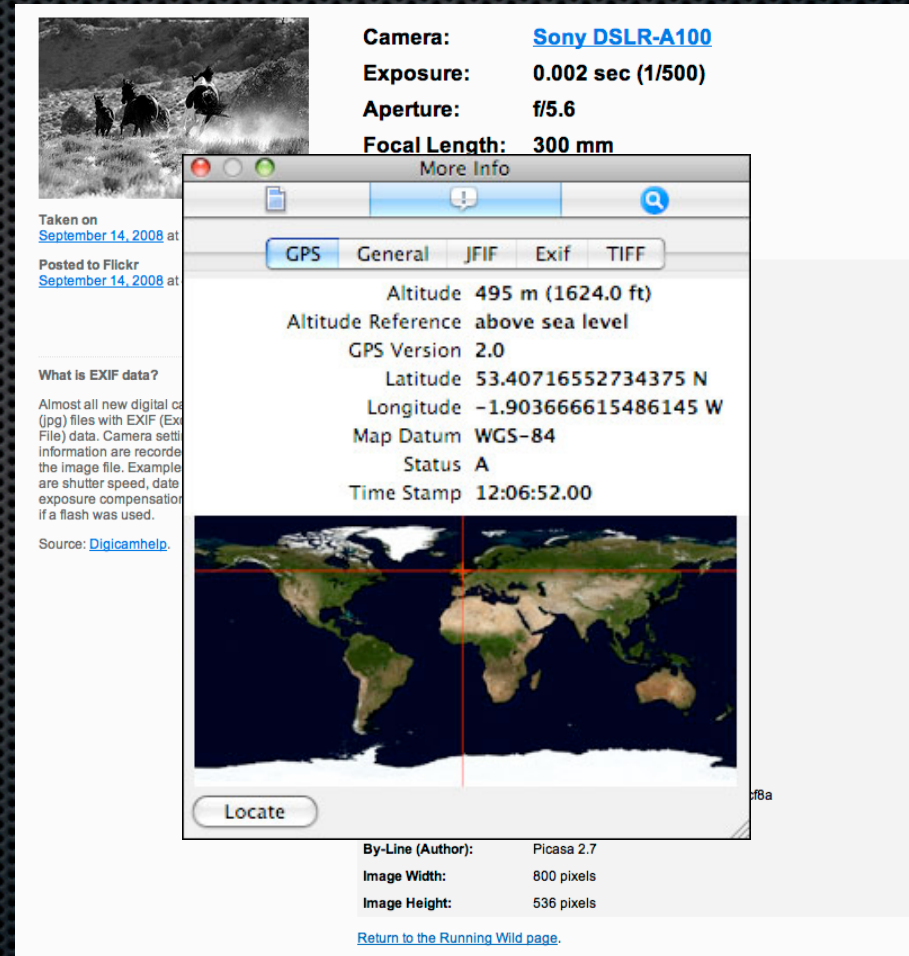
:/



# 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.



The screenshot displays an online EXIF viewer interface. At the top left is a thumbnail of a photo showing several horses running through a field. To the right of the thumbnail, the following camera metadata is listed:

- Camera: [Sony DSLR-A100](#)
- Exposure: 0.002 sec (1/500)
- Aperture: f/5.6
- Focal Length: 300 mm

Below the camera info, a 'More Info' window is open, showing tabs for GPS, General, JFIF, Exif, and TIFF. The 'GPS' tab is selected, displaying the following location data:

- Altitude: 495 m (1624.0 ft)
- Altitude Reference: above sea level
- GPS Version: 2.0
- Latitude: 53.40716552734375 N
- Longitude: -1.903666615486145 W
- Map Datum: WGS-84
- Status: A
- Time Stamp: 12:06:52.00

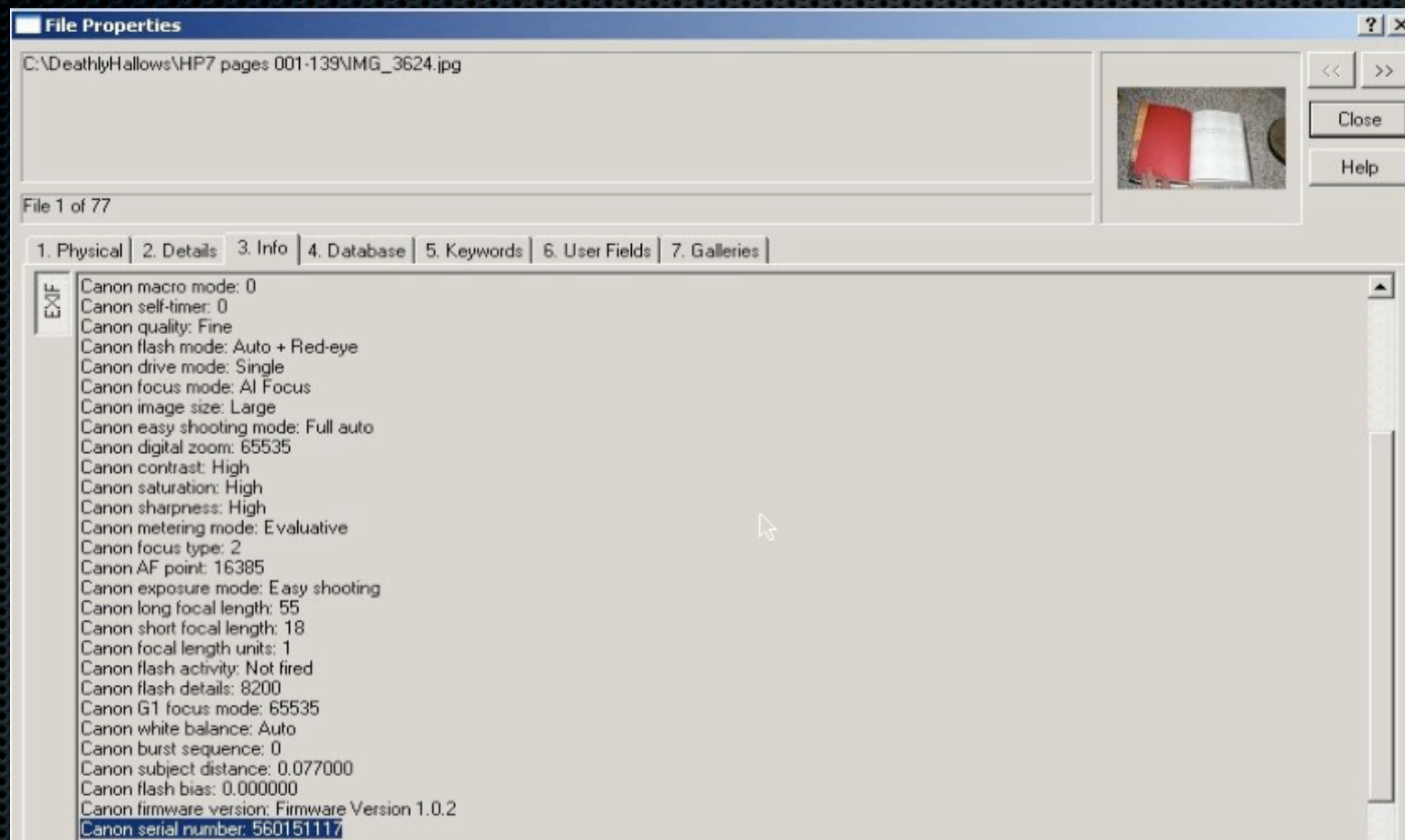
Below the GPS data is a world map with a red crosshair indicating the location. A 'Locate' button is positioned at the bottom left of the map. To the right of the map, the following image metadata is shown:

- By-Line (Author): Picasa 2.7
- Image Width: 800 pixels
- Image Height: 536 pixels

At the bottom of the page, there is a link: [Return to the Running Wild page.](#)



# Metadata - EXIF- Harry Pwner



## Deathly EXIF?



# Cat Schwartz - Tech TV



FAIL





# Metadata

- ✦ Modification and retouched photos
- ✦ Descriptions of photos
- ✦ Plagios
- ✦ Copy & paste



# Metadata

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



# Metagooofil

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





# Metagoofil

User names

Workers  
names

Server names

Paths

Software  
versions + Date

Mac Address





# Metagoofil

- ✦ Document copy & paste
- ✦ Authors
- ✦ Edition time
- ✦ Printer used
- ✦ Comments
- ✦ Revisions



# Metagoofil

site:nasa.gov filetype:ppt

The screenshot shows a Google search interface with the query 'site:nasa.gov filetype:ppt' entered in the search bar. The search results are displayed under the 'Web' tab. The first result is titled '[PPT] Annual Procurement Report' and is a Microsoft Powerpoint file. The second result is titled '[PPT] www.nasa.gov/ppt/47355main\_Headquar.ppt' and is also a Microsoft Powerpoint file. The third result is titled '[PPT] MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE' and is a Microsoft Powerpoint file. The fourth result is titled '[PPT] www.nasa.gov/ppt/119097main\_Marks.ppt' and is a Microsoft Powerpoint file. The fifth result is titled '[PPT] www.nasa.gov/ppt/118984main\_heymsfield\_telcon\_slid...' and is a Microsoft Powerpoint file.

Google Web Images News Maps <sup>New!</sup> 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](#)

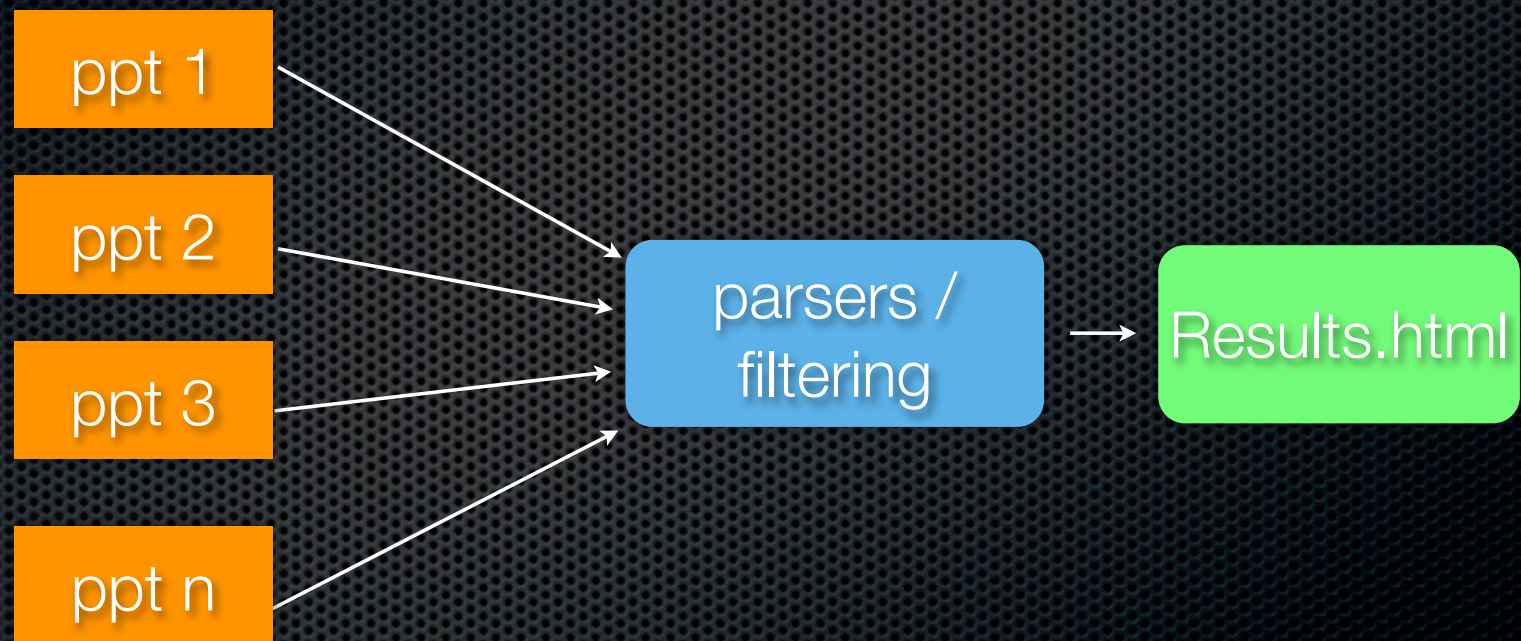
[\[PPT\] www.nasa.gov/ppt/119097main\\_Marks.ppt](#)  
File Format: Microsoft Powerpoint - [View as HTML](#)  
1. NOAA 2005 Hurricane Field Program — Intensity Forecast Experiment (IFEX) Frank Marks  
NOAA/AOML Hurricane Research Division ...  
[Similar pages](#)

[\[PPT\] 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 ...



# Metagoo<sub>o</sub>fil

Downloaded files





# Metagoofil - results

[http://lwsscience.gsfc.nasa.gov/Townsend\\_LWSWG.ppt](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](http://saber.larc.nasa.gov/03SABER_non_LTE_algo_approach.ppt)

Local copy, failed download :(

[http://ldcm.nasa.gov/library/Analysis\\_L7ImageryPurchases\\_110501.ppt](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/IMDCPework.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](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](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](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_PMSEP
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.doc
revision history - Revision #5: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-9-02.doc
revision history - Revision #4: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02.doc
revision history - Revision #3: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02.doc
revision history - Revision #2: Author 'Edutech User' worked on 'C:\WINDOWS\Temporary Internet Files\OLK4\PMSEP De
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:

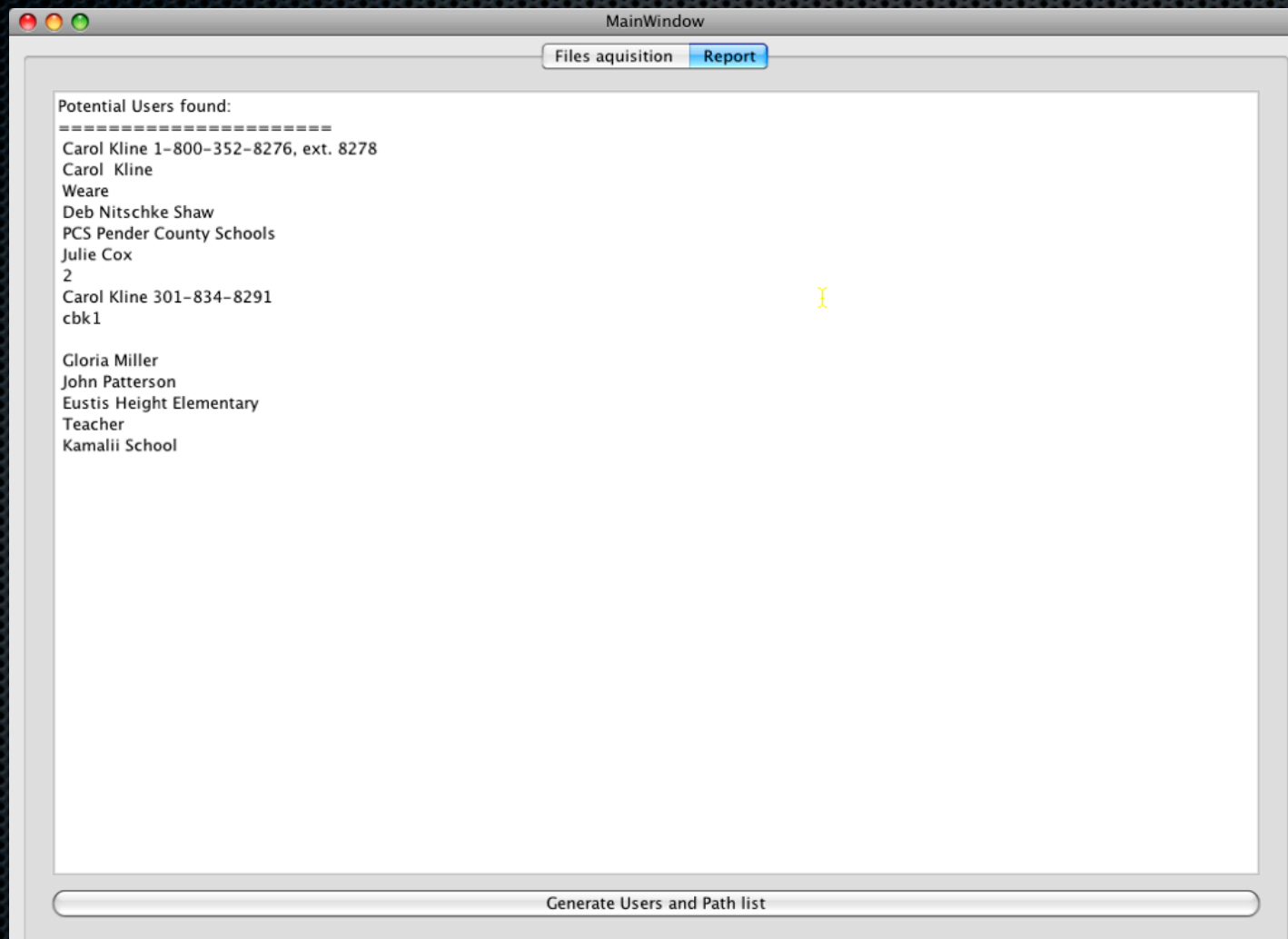
```
C:\Documents and Settings\baltner\Application Data\Microsoft\Word\  
C:\_ISEM\MyProjects\XMLCIO\projectPlan\  
C:\Documents and Settings\rbenedic\My Documents\XML\NASA XML\XML Business Case\Final Business Case\  
  
Normal\  
C:\WINNT\Personal\  
\br/>U:\users\smarucci\A1\Writing\Internet\HOMEPAGE\cs\  
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  
\\RGINTS\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:\br/>A:\br/>C:\Documents and Settings\akennedy\My Documents\Data\attach\  
U:\users\kbayer\DATA\Word\  
Macintosh HD:Users:mls: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\
```



# Metagoogle - results



# Metagoofil v2





# Metagoofil & Linkedin results

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



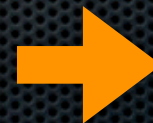
# Using results

- ✦ 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, Linkedin, Website
- ✦ People search:



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



# People search

spokeo™

**spokeo™**

Enter a friend's email or personal website **SEARCH** [Import my Friends](#)

e.g. name@domain.com, www.myspace.com/name or any RSS feed

[Settings](#) | [Invite](#) | [Log Out](#)

**Friends** [» Edit](#)

▼ **FREE RESULTS**

- ▶ **cmartorella@edge-security.com** 3
- ▶ laramies

▼ **PREMIUM RESULTS**

- 🔒 vicente.diaz@gmail.com
- 🔒 Vicente Diaz
- 🔒 **cmartorella@edge-security.com** 3
- 🔒 trompeti

**Recent Updates**

YouTube

webshots

digg

facebook

LinkedIn

NETLOG

slide

flickr

StumbleUpon

MULTIPLY

veoh

Picturetrail

myspace

hi5

gebo

amazon.com

photoBuddie

!

VIDEO

imeem

twitter

yelp

Picasa

Windows Live Spaces

friendster

xanga

PANDORA

BUZZNET

Blogger

VOX

Flixster



# People search

spokeo™

**spokeo™**

e.g. name@domain.com, www.myspace.com/name or any RSS feed


**SEARCH**


[Import my Friends](#)

[Settings](#) | [Invite](#) | [Logout](#)


**Friends** [» Edit](#)


**FREE RESULTS**


 [cmartorella@edge-security.com](#) 3


 [laramies](#)

**PREMIUM RESULTS**


 [vicente.diaz@gmail.com](#)

 [Vicente Diaz](#)


 [cmartorella@edge-security.com](#) 3

 [trompeti](#)

**laramies** [» Show Recent Updates](#)

 **SQL Server Forensic Analysis**

February 01, 2009 on Amazon



Usually ships in 24 hours


Date Added: 2009-02-01

Desired: 1

Received: 0


Sales Rank: 503165

Price: **\$38.49**

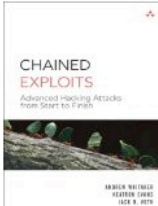


7 used and 28 new from \$29.97

[share](#)

 **Chained Exploits: Advanced Hacking Attacks from Start to Finish**

February 01, 2009 on Amazon



Not yet published


Date Added: 2009-02-01

Desired: 1

Received: 0


Sales Rank: 76206

Price: **\$31.19**



1 new from \$31.19

[share](#)


 **laramies's profile**

January 12, 2009 on Picasa

**Nickname**

laramies

[share](#)

 **Video "Google Email Harvester 0.3 Presentation" | sevenload**

December 28, 2008 on Web Results

... 0.3 #Todo:salida con formato, filter=0 #by laramies@gmail.com Edge-security #Christian Martorella ... Um Videos bei sevenload ansehen zu können wird der Adobe ...

[share](#)



# People search



Browser tabs: Techie worki..., Command Li..., Metasploit..., 10 Privacy Se..., SANS Interne..., Multimedia, Monthly Bri..., Christian Martorella, Barc...

Address bar: <http://www.pipl.com/search/?FirstName=christian&LastName=martorella&City=barcelona&State> Google

Google Maps Send to Coccolicious

**pipl** Name Email Username Phone

christian martorella barcelona ES Search Clear

First Name Last Name City State Country

**Christian Martorella, Barcelona, Spain**

No results found for Christian Martorella, barcelona, Spain

Suggestions:

- Make sure the words are spelled correctly.
- Try searching with other parameters.
- Try searching in other categories.

Results for Christian Martorella without Spain

**Quick Facts**  
Christian Martorella has been working in the field of information security for the last 10 years, starting his career in Argentina IRS as security... [www.sourceconference.com](http://www.sourceconference.com)

**Personal Profiles**

- Christian Martorella...**  
Personal Web Profile - Facebook [www.facebook.com](http://www.facebook.com)
- Christian Martorella...**  
Personal Web Profile - Facebook [www.facebook.com](http://www.facebook.com)
- Christian Martorella...**  
Customer Profile - Amazon.com [www.amazon.com](http://www.amazon.com) - Deep Web

Sponsored Tip: Find hidden profiles and photos across MySpace, Facebook and 40+ networks... [www.spokeo.com](http://www.spokeo.com)

**Publications**

- [ Full-disclosure ] [ Tool ] - Metagoofil. Secure-Computing, - Last post: Aug 28, 2007...**  
Messages - Google Groups [groups.google.com](http://groups.google.com)
- RBL not working. mailing.postfix.users, - 1 post - 1 author - Last post: Mar 16,...**  
Messages - Google Groups [groups.google.com](http://groups.google.com)

**Email Address**

- ... S21Sec - Christian Martorella <cmartorella@s21sec.com> S21Sec [ REFERENCES ] \***  
FCKeditor <http://www.fckeditor.net> \* S21Sec <http://www.s21sec.com>  
S21Sec Advisory ... [www.s21sec.com](http://www.s21sec.com)
- From: Christian Martorella (cmartorella\_at\_isecauditors.com). Date: 06/09/05 ... Christian Martorella e-Security Engineer cmartorella@isecauditors.com ...**  
SecurityFocus Penetration: Re: SQL Injection [www.derkeiler.com](http://www.derkeiler.com)
- Advanced web application defense with Modsecurity. Daniel Fernandez Bleda dfernandez@isecauditors.com. Christian Martorella cmartorella@isecauditors.com.**  
Advanced Web Application Defense with ModSecurity [wiki.whatthehack.org](http://wiki.whatthehack.org)

**Web Pages** web and image results enhanced by Google™

- Christian Martorella. Gender: Male; Industry: Technology; Occupation: Security Engineer; Location: Barcelona : Catalunya : Spain ...**  
Blogger: User Profile: Christian Martorella [www.blogger.com](http://www.blogger.com)
- Aug 27, 2007 ... From : Christian Martorella <laramies2k\_at\_yahoo.com.ar> ... Regards,.**

**Sponsored Links**

- Defend Your Reputation**  
Search & Destroy Misleading Info.  
Get your free trial now.  
[ReputationDefender.com](http://ReputationDefender.com)
- Promote Your Name**  
Control What People See When They Search Your Name On The Web  
[LookupPage.com](http://LookupPage.com)

Give Feedback



# Usercheck.com

USERNAME:

12seconds - available	ILikeTotallyLovelt - 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	Ttpd - available
Corkd - available	Kwippy - available	Tipjoy - available
Dailymotion - available	Lastfm - taken	Tumblr - available
Delicious - taken	LinkedIn - available	Twitter - available
Digg - available	Livejournal - taken	Typed - available
Diigo - taken	Magnolia - available	Usvoice - 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
Pfffound - 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
Helloxtxt - available	Pownce - available	Yotify - available
Hexday - available	Rejew - available	Youtube - taken



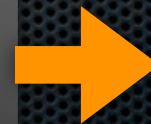
# Using results

- ✦ Password profiling

Dictionary creation: words from the different user sites



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



**Brute force  
ATTACK**



# Microblogs

yammer

twitter



- ✦ Microblogging
- ✦ Small posts up to 140 characters





## BarackObama

[Follow](#)

is asking you to honor Dr. Martin Luther King, Jr by volunteering in your area. Visit <http://USAservice.org> or text SERVE to 56333 for info.

1:01 PM Jan 19th from web

To participate in the Inauguration visit <http://pic2009.org> or text HISTORY to 56333. Follow the Inauguration on Twitter @obamainaugural

5:52 PM Jan 15th from web

We just made history. All of this happened because you gave your time, talent and passion. All of this happened because of you. Thanks

9:34 AM Nov 5th, 2008 from web

Asking you to help Get Out the Vote in these last few critical hours of our campaign for change. Visit <http://my.barackobama.com/f...>

12:42 PM Nov 4th, 2008 from web

**Name** Barack Obama

**Location** Chicago, IL

**Web** <http://www.barack...>

351,687  
following

371,430  
followers

265  
updates

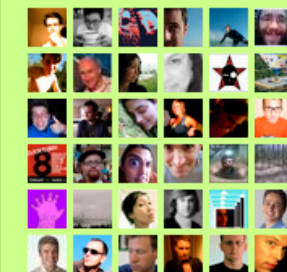
### Updates

### Favorites


### Actions

[block](#) BarackObama

### Following



[View All...](#)

 [RSS feed of BarackObama's updates](#)





## 5k Twitter Browser by Neuro Productions

Instructions: Fill in a twitter username and start clicking and dragging.

Username:

New only: ☐

Fullscreen: ☐



kornbrust

<http://www.hud.ws/0v3>



tqbf

@gruber --- Ebert already gave it a strong review...



dakami

@dinodaizovi @alexstirov



41414141



van



acores



LilRed\_Apaqo



searchio



secobis



Marsmen



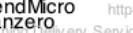
sundejohnson



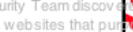
CoreSecurity



ITPRO



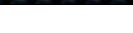
SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secwest



esizkur



laramies



erma



o\_o



PROJECT HAKER HISTORIA



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson



CoreSecurity



ITPRO



SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson



CoreSecurity



ITPRO



SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson



CoreSecurity



ITPRO



SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson



CoreSecurity



ITPRO



SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson



CoreSecurity



ITPRO



SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson



CoreSecurity



ITPRO



SCMagazine



TrendMicro



deanzero



dojosec



ryanaraine



dildoq



druidian



timoreilly



alexstirov



impesp



nicowaisman



CaliDeals



svpn



ricardobruno



secobis



Marsmen



sundejohnson





# Bookmarks



Search all of Delicious for 192.168.1

Everybody's bookmarks 304 results - show all

<a href="http://192.168.1.1/cgi-bin/webcm">http://192.168.1.1/cgi-bin/webcm</a> SAVE	113
First saved by: djtrees	router modem adsl internet aztech
<a href="http://192.168.1.2">192.168.1.2</a> SAVE	110
First saved by: jacklarge	hardware router computer music asus
<a href="http://192.168.1.103/">http://192.168.1.103/</a> SAVE	21
First saved by: arrigo	100 firefox:bookmarks home imprimante informatique
<a href="http://192.168.1.102/">http://192.168.1.102/</a> SAVE	30
First saved by: Briana	iphone network online printer printers
<a href="http://192.168.1.100">http://192.168.1.100</a> SAVE	61
First saved by: meerkat_wx	network apache computer download hardware
<a href="http://root:clubadmin@192.168.1.1/scsncr...?action=view">http://root:clubadmin@192.168.1.1/scsncr...?action=view</a> SAVE	2
First saved by: mike72	ip reseau router
<a href="http://192.168.1.251/">http://192.168.1.251/</a> SAVE	5
First saved by: phamlong	router datos homenetwork network red
<a href="http://192.168.1.33">192.168.1.33</a> SAVE	11
First saved by: solkar_saruman	2500 anto communication diskstation emule
<a href="http://192.168.1.1/home.html">http://192.168.1.1/home.html</a> SAVE	4
First saved by: finni999	amper broadband herramientas_sistema modem myfav-firefox
<a href="http://192.168.1.51/">http://192.168.1.51/</a> SAVE	7
First saved by: blacjax	cars konr.ad musicpal sligolan system

Everyone's Related Tags

router network modem computer hardware



facebook

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



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



facebook



**Was shown the door after posting that her job was  
'boring' on her Facebook page**



# More than meet the eyes



33663  
Q1 08

7.37. car  
series

PAPERS FOR  
CABINET MEETING  
13 MAY 2008

CT  
Housing  
Support  
Unit

Caroline Flint – Speaking Notes

### State of Housing market

- Colleagues will know the 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:



# Real life I.G example

- ✦ Looking for a Housekeeper on Craigslist
- ✦ 3 interesting resumes came up:

Myspace page, applicant drinking beer from a funnel

Personal blog, saying that she is applying for menial jobs, and will quit as soon she sells some paintings

Local police, applicant arrested 2 years before for shoplifting



# 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, all stay online
- ✦ Think twice what you post
- ✦ Check the privacy configuration of your tools/sites



# References

- ✧ [www.edge-security.com](http://www.edge-security.com)
- ✧ [blog.s21sec.com](http://blog.s21sec.com)
- ✧ [www.s21sec.com](http://www.s21sec.com)
- ✧ [carnal0wnage.blogspot.com](http://carnal0wnage.blogspot.com)
- ✧ [www.gnunet.org/libextractor](http://www.gnunet.org/libextractor)
- ✧ [lcamtuf.coredump.cx/strikeout/](http://lcamtuf.coredump.cx/strikeout/)
- ✧ [www.paterva.com](http://www.paterva.com)
- ✧ [http://sethgodin.typepad.com/seths\\_blog/2009/02/personal-branding-in-the-age-of-google.html](http://sethgodin.typepad.com/seths_blog/2009/02/personal-branding-in-the-age-of-google.html)



# References II

[http://www.neuroproductions.be/  
twitter\\_friends\\_network\\_browser/  
laramies.blogspot.com](http://www.neuroproductions.be/twitter_friends_network_browser/laramies.blogspot.com)



?





**Tomorrow's Digital Security, Today**

Thank you for coming

[cmartorella@s21sec.com](mailto:cmartorella@s21sec.com)

[cmartorella@edge-security.com](mailto:cmartorella@edge-security.com)

<http://laramies.blogspot.com>

<http://twitter.com/laramies>