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

S21sec
Tomorrow's Digital Security, Today

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

S21sec

Tomorrow's Digital Security, Today

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?

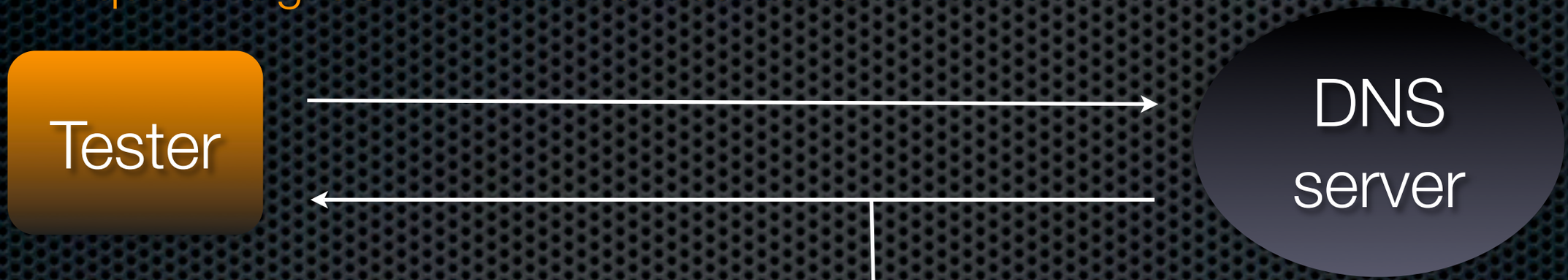
S21sec
Tomorrow's Digital Security, Today

Obtaining host and Domains info - Classic

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

Zone-Transfer - DIG

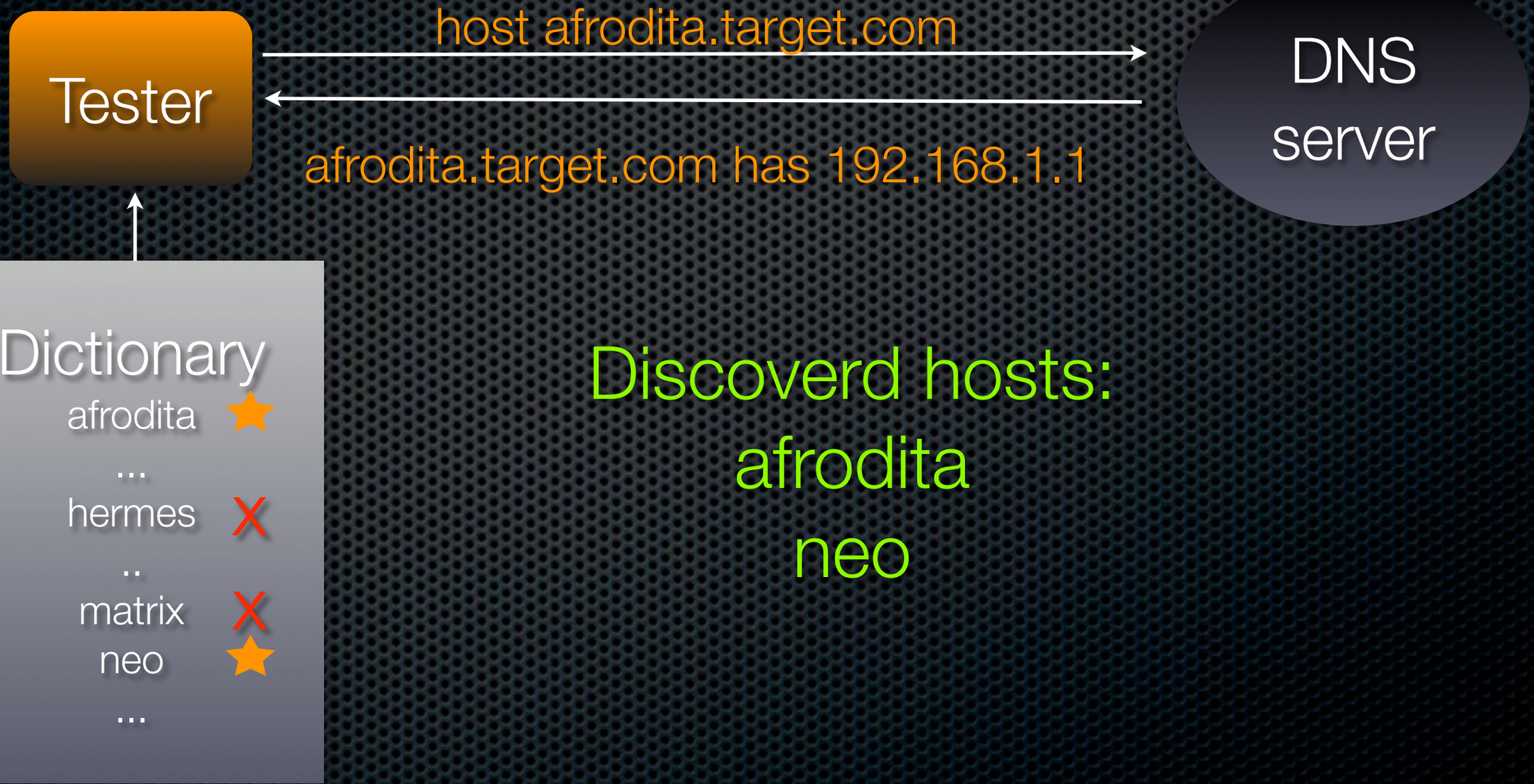
request: dig @srv.weak.dns weak.dns -t AXFR




```
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



Discoverd hosts:
afrodita
neo

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 ...

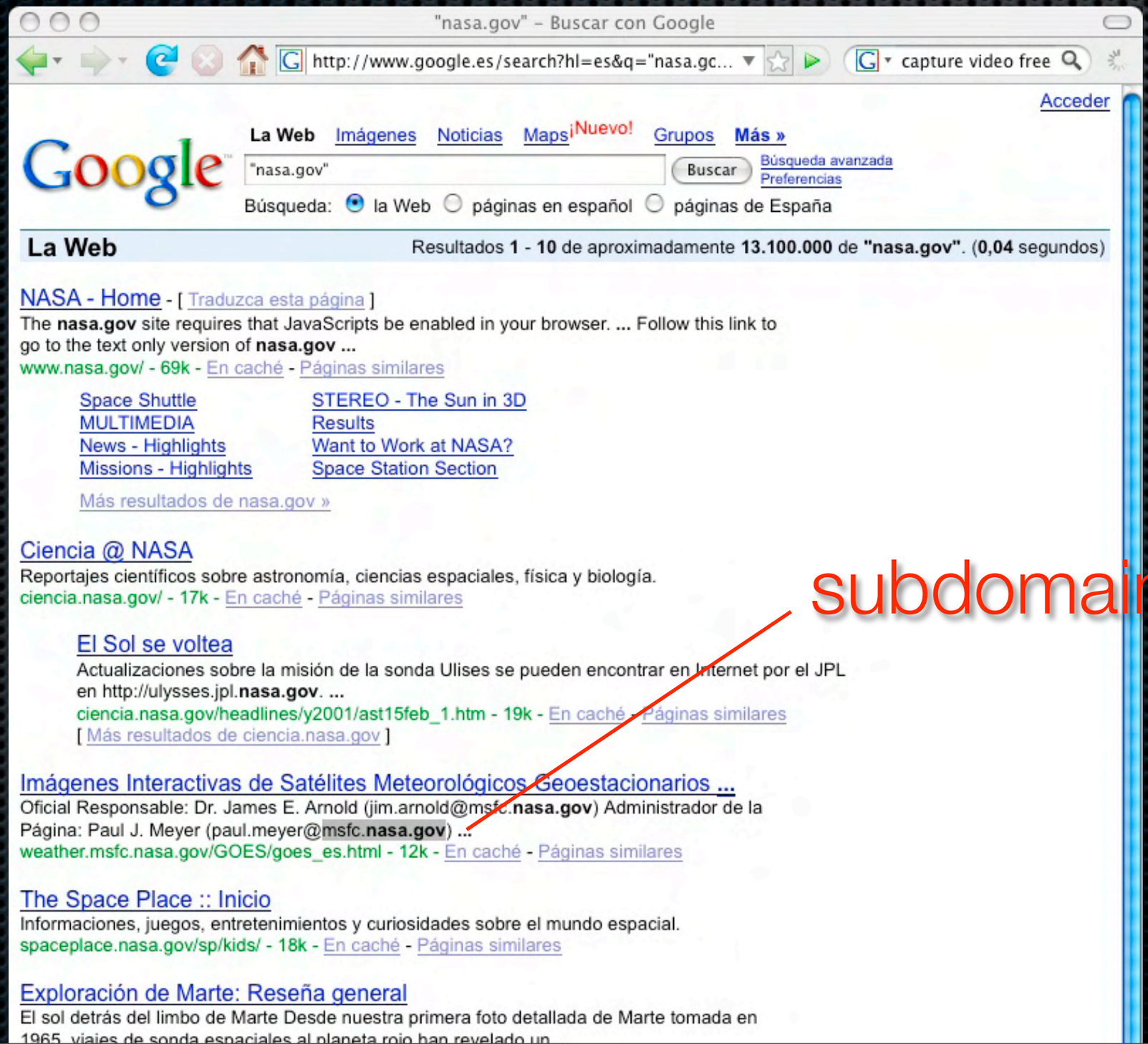
S21sec

Tomorrow's Digital Security, Today

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**



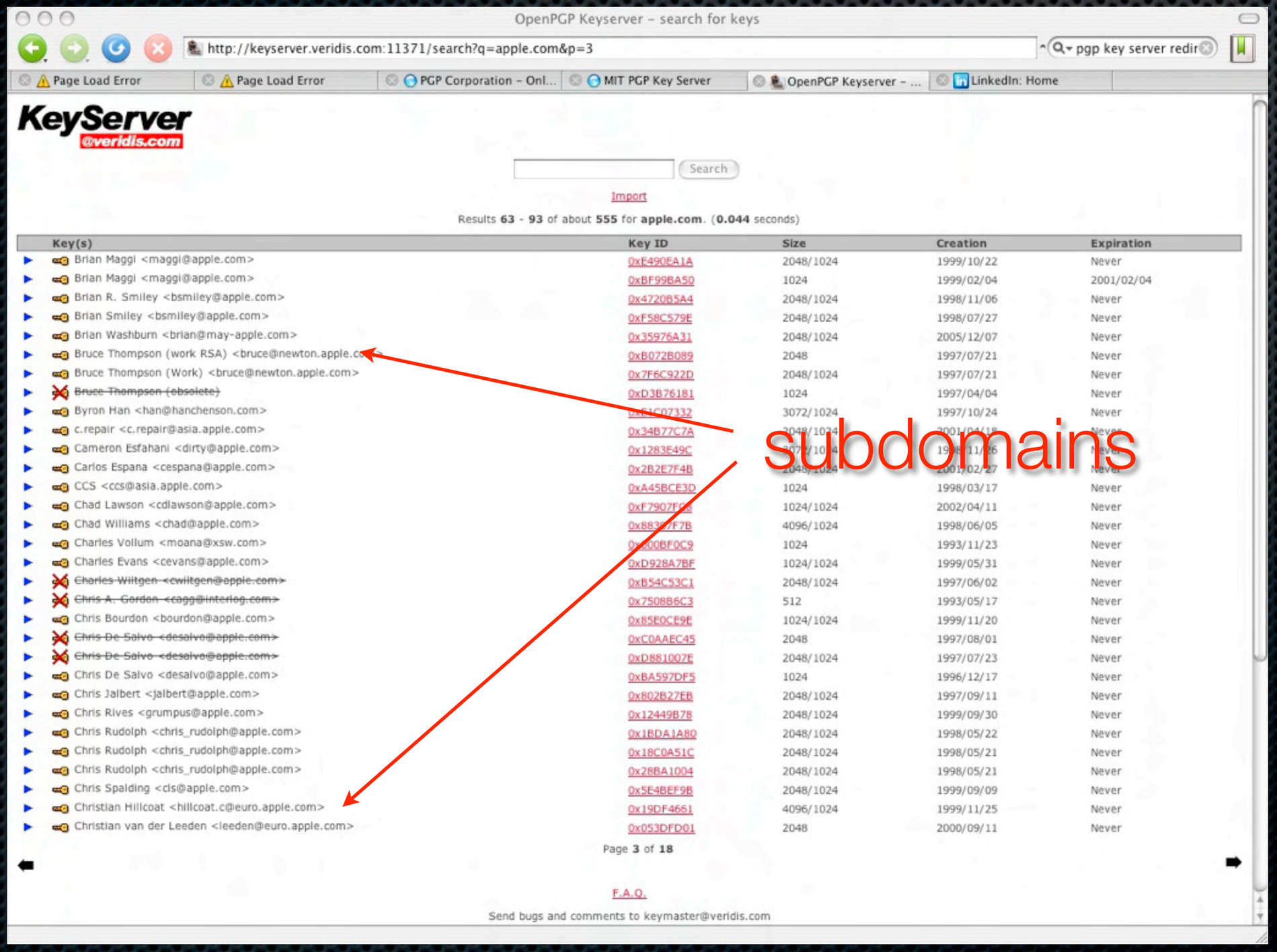
Obtaining host and Domains info

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

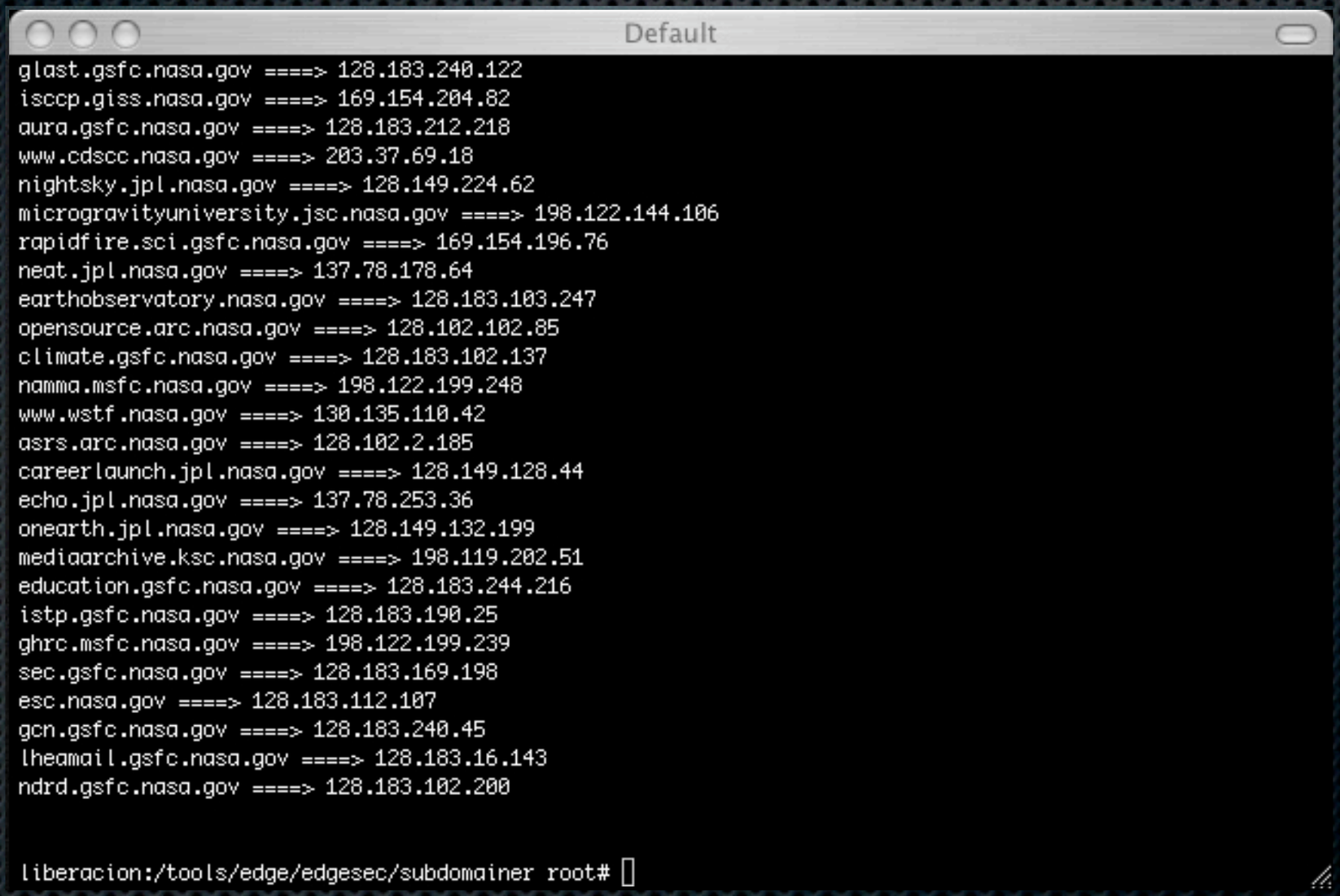
http://keyserver.veridis.com/

http://pgp.rediris.es:11371/pks/lookup?search=domain

Obtaining host and Domains info



Obtaining host and Domains
Subdomainer



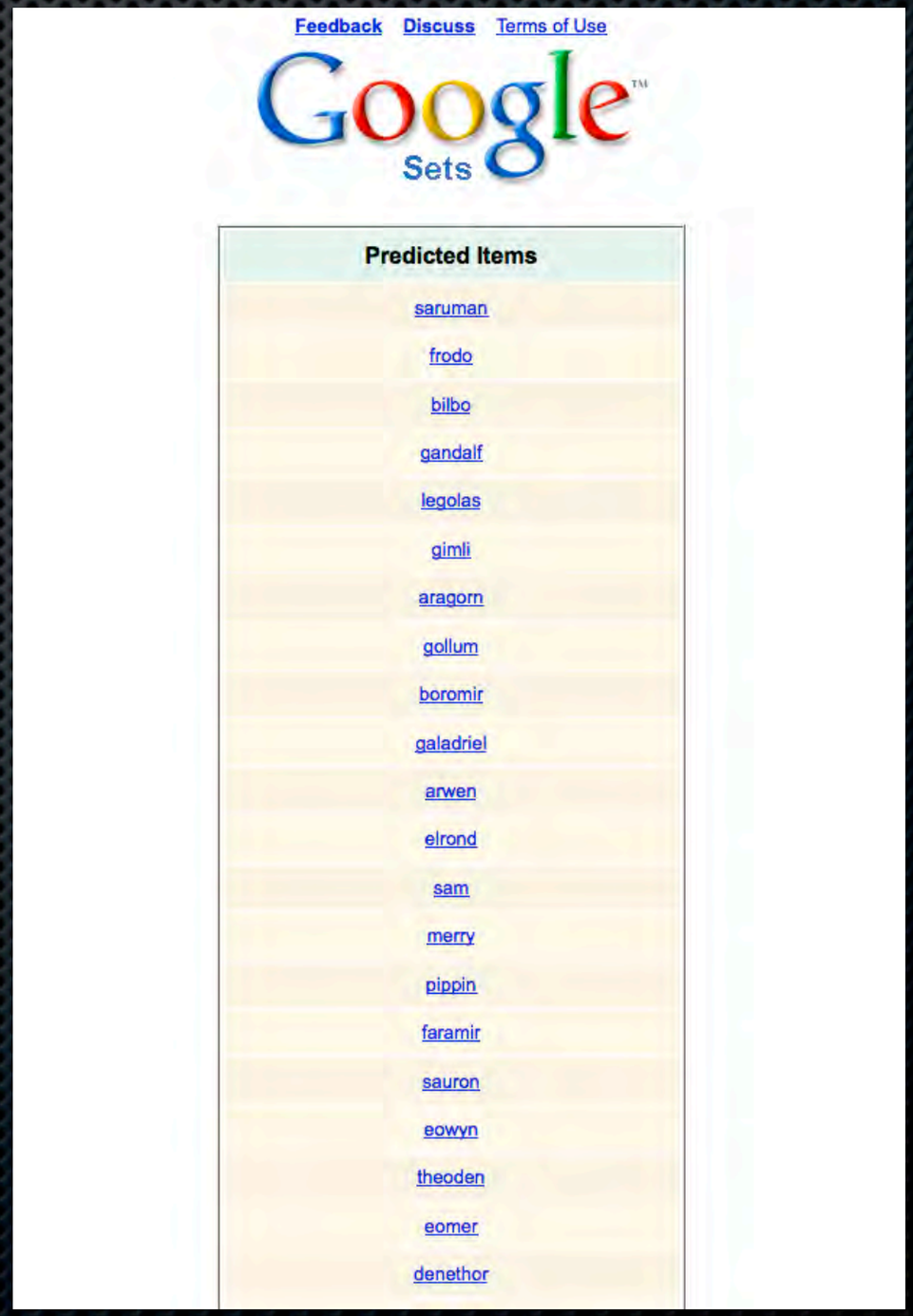
S21sec
Tomorrow's Digital Security, Today

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



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

Obtaining user info - New sources

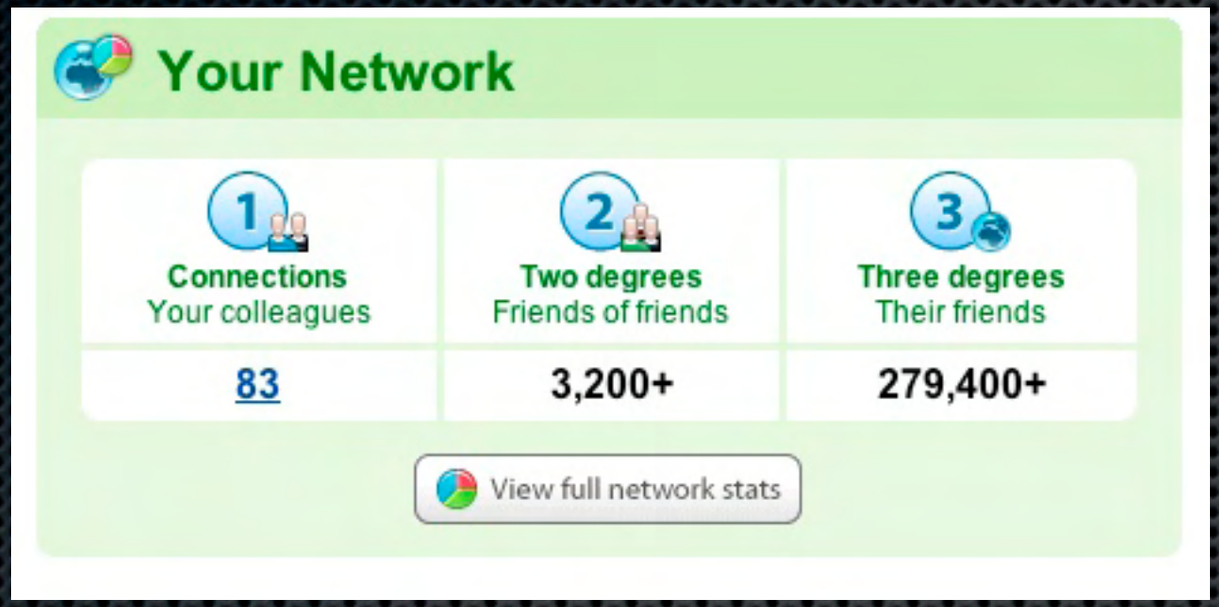
- PgP key servers (passive)
- Social Networks (passive)
- Metadata (passive)

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

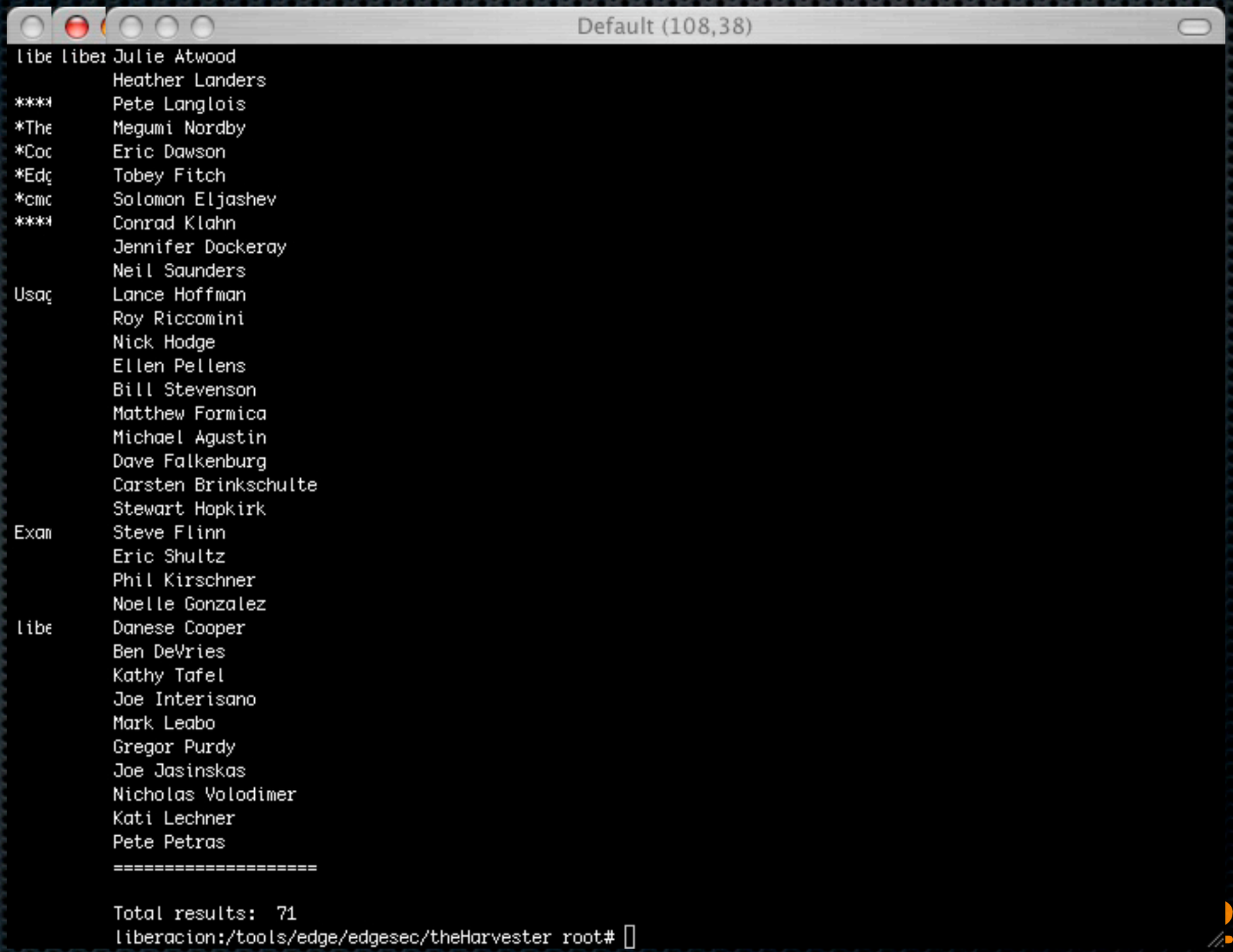


Current Job
Pasts Jobs
Education
Job description
Etc...

S21sec
Tomorrow's Digital Security, Today

Obtaining user info - New sources

Obtaining user info - theHarvester



Obtaining Emails - theHarvester

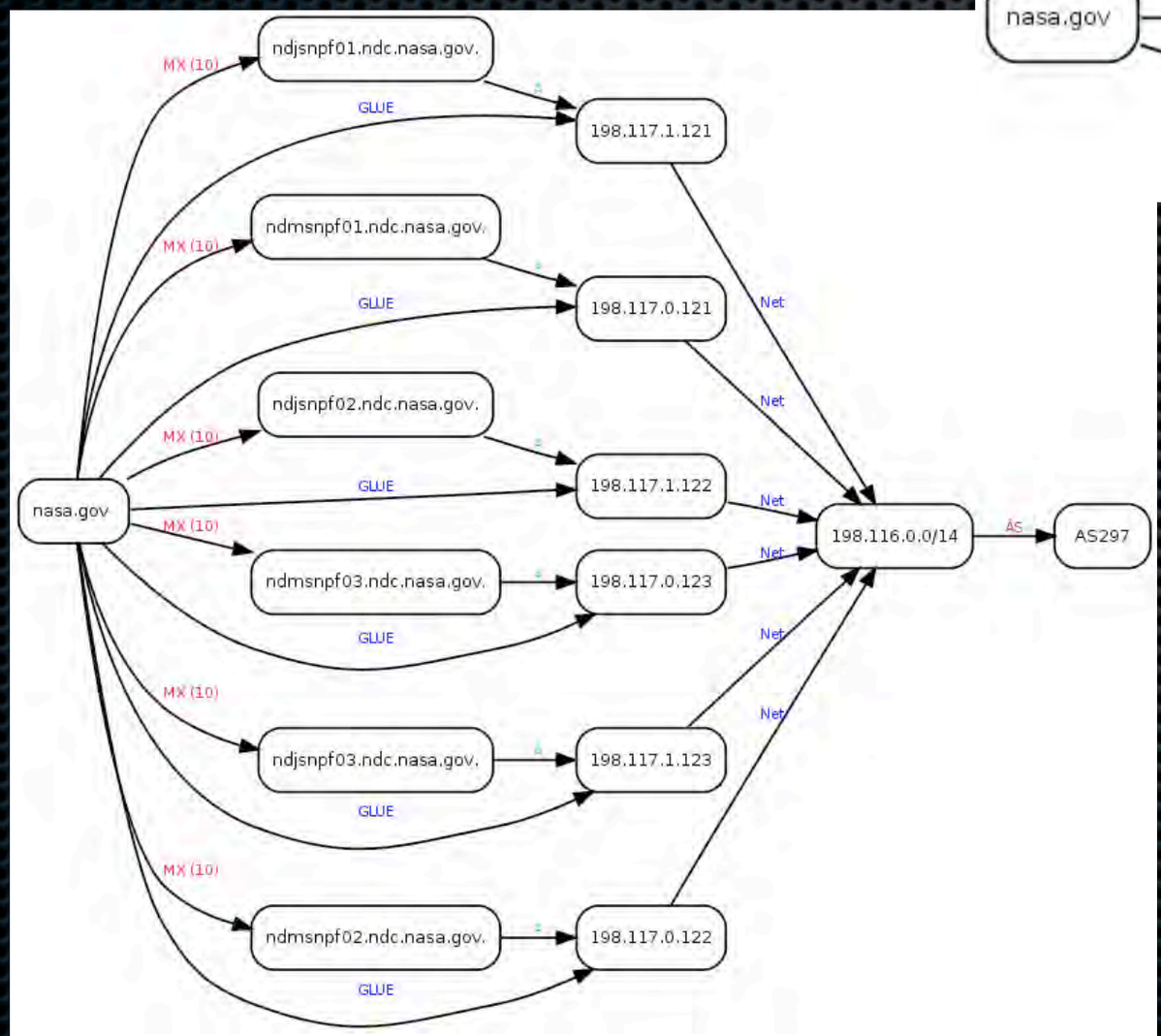
Default (108,38)

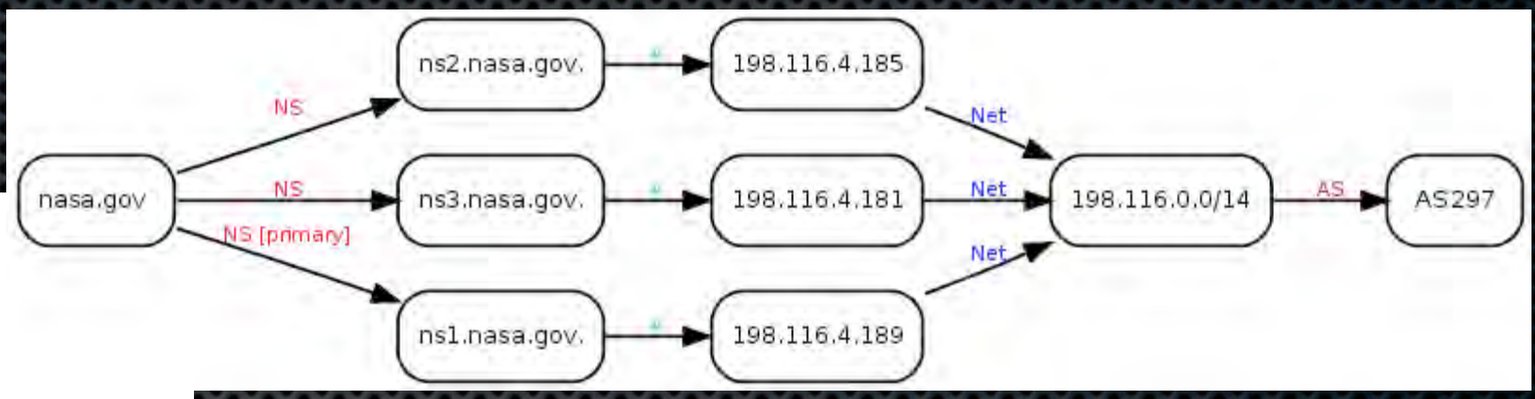
```
liberacion:/tools/edge/edgesec/theHarvester root# python theHarvester.py -d "nasa.gov" -l 100 -b google

*************************************
*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.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#
```

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

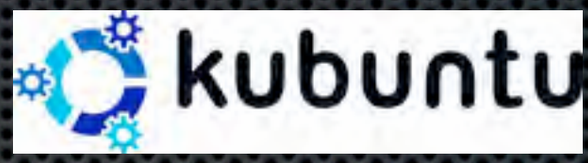
Provides basic information such as the author of a work, the date of creation, links to any related works, etc.

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

lo png



logo-Kubuntu.png

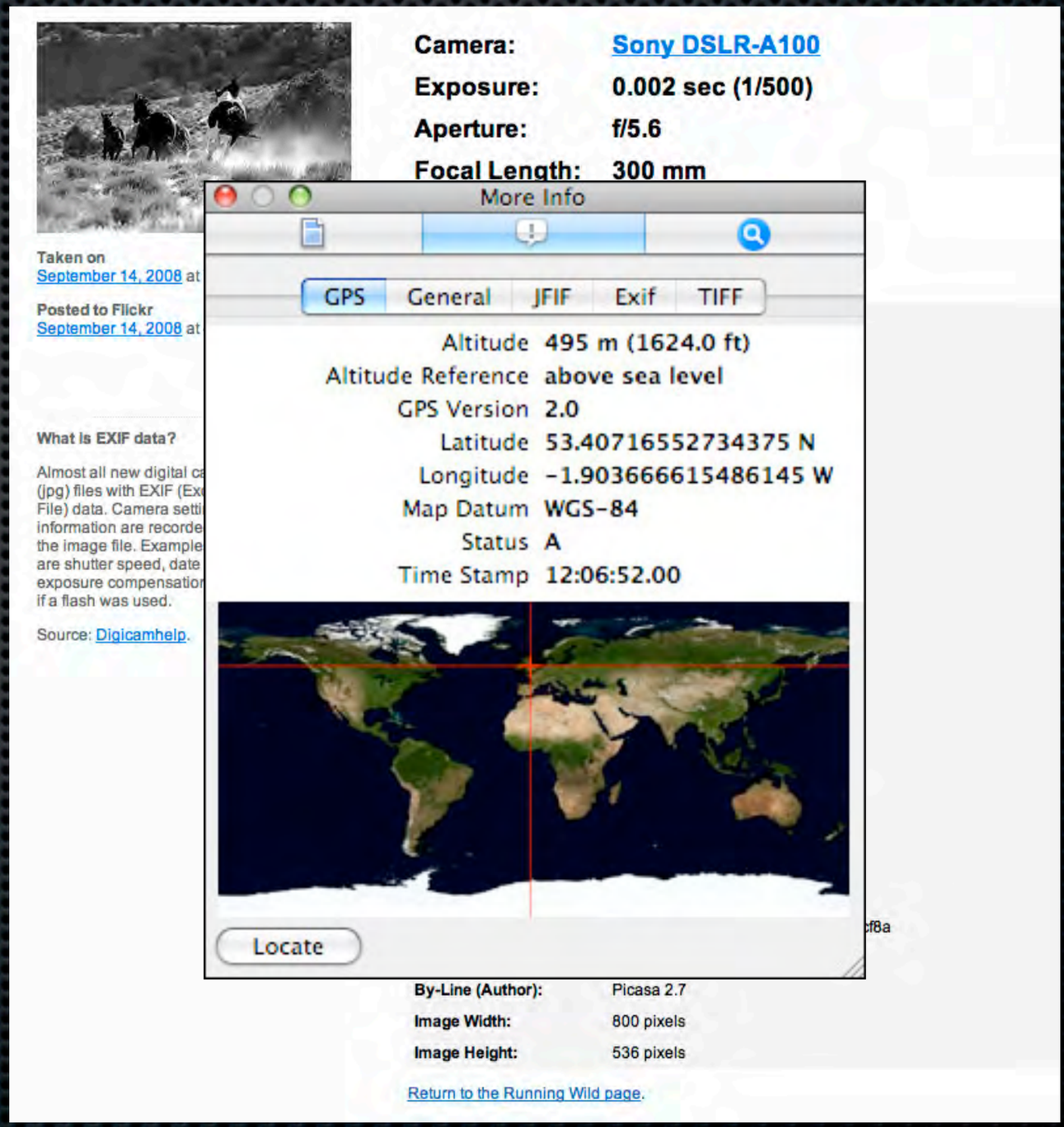
software - Adobe ImageReady
size - 1501x391
mimetype - image/png

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

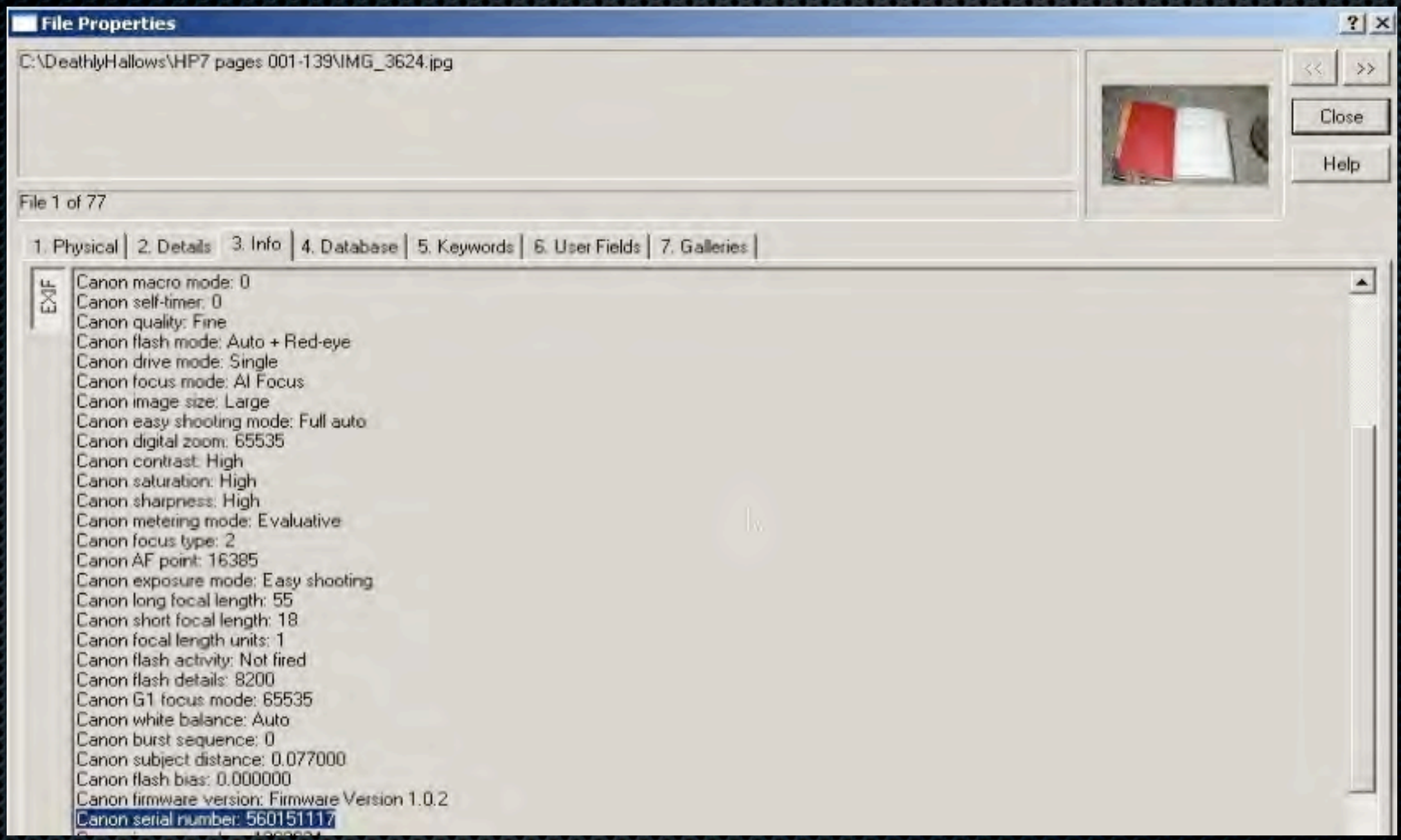
:/

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.



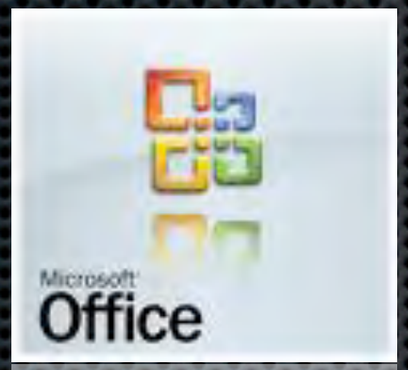
Metadata - EXIF- Harry Pwner



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.

S21sec
Tomorrow's Digital Security, Today

Metagoofil

User names

Workers names

Server names

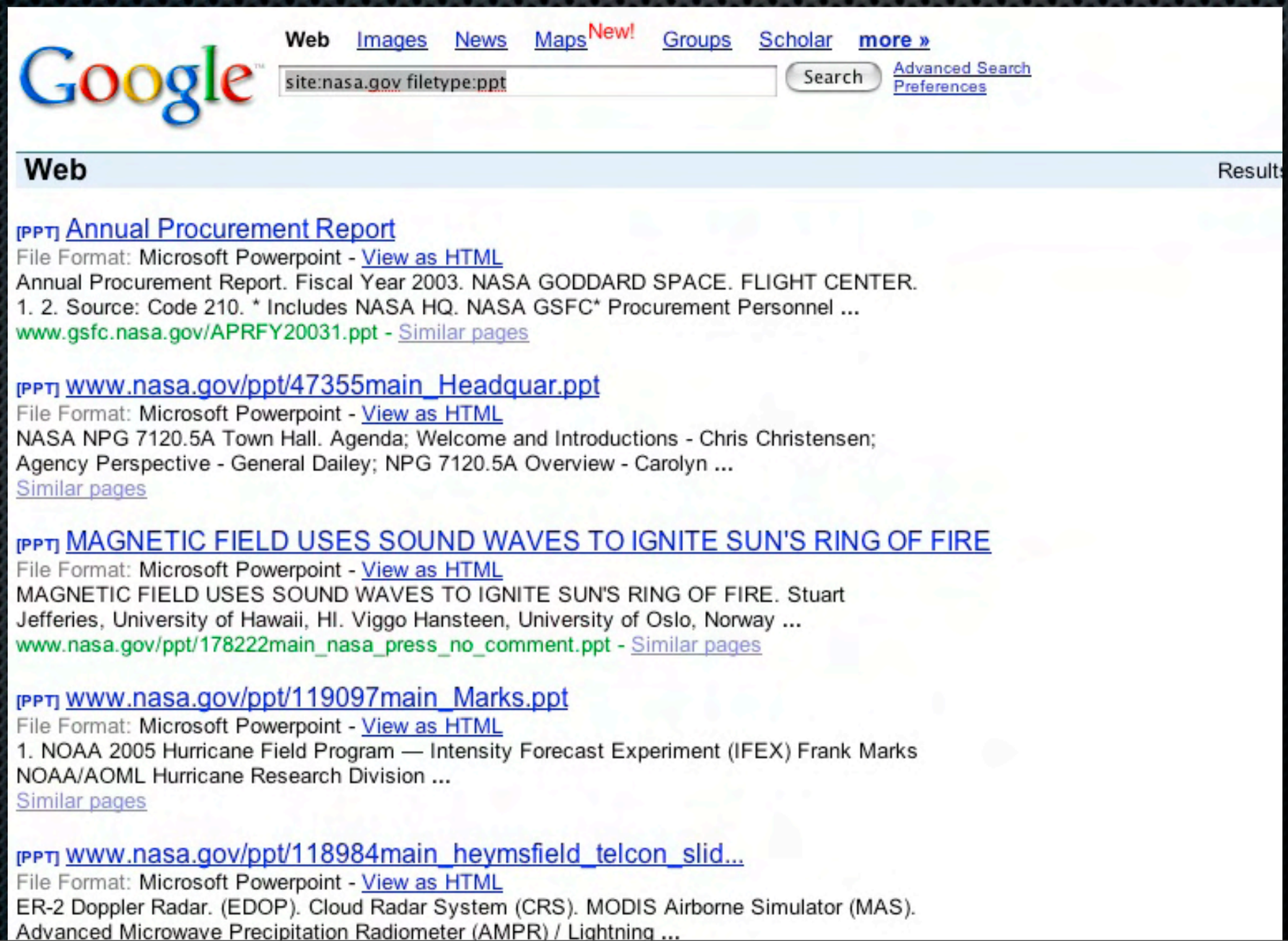
Paths

Software versions + Date

Mac Address

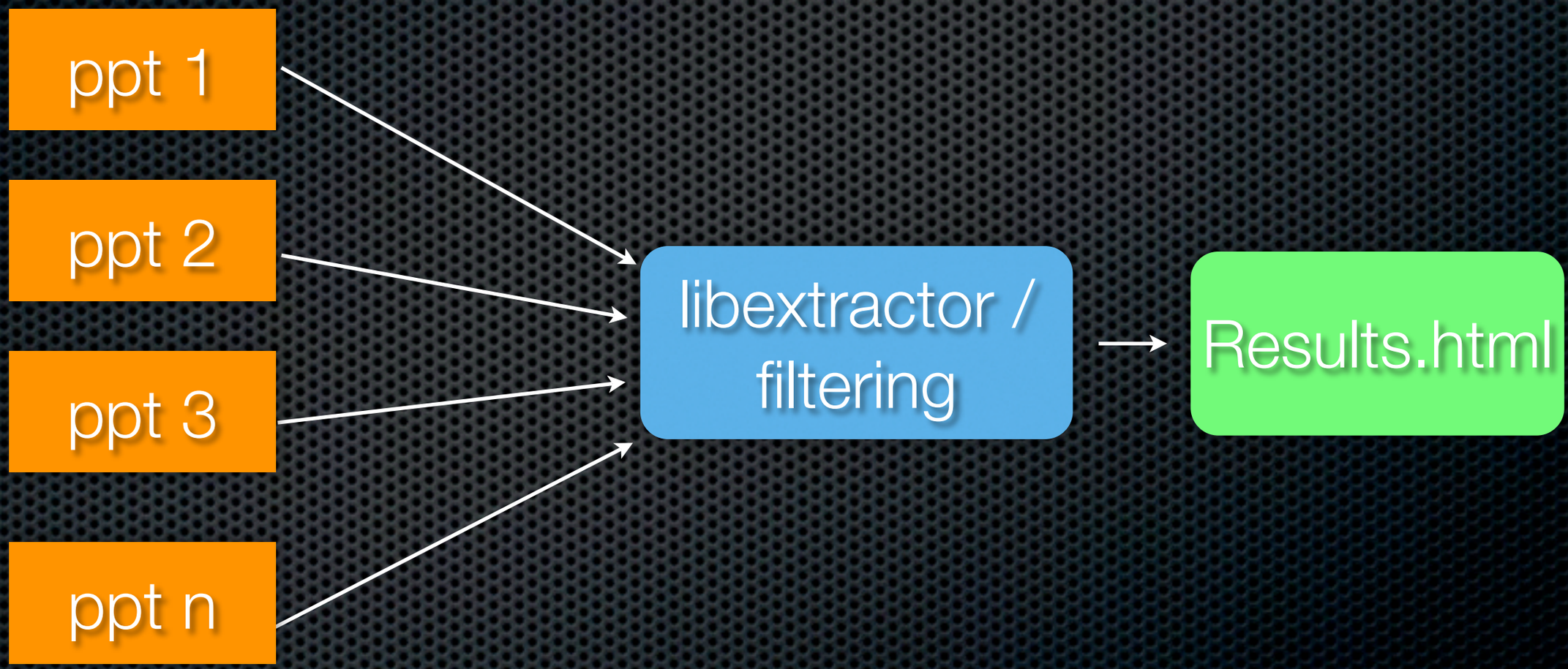
Metagoofil

site:nasa.gov filetype:ppt



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\ml0282\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 Structu
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.
revision history - Revision #5: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-9-02.
revision history - Revision #4: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02.
revision history - Revision #3: Author 'Edutech User' worked on 'C:\My Documents\PMSEP Detailed Structure 8-7-02.
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\Al\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 Revisior
\\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:\
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\
```

Metagoofil - results

RÃ¥Ã½Â¼9RÂ¦8\\nÂ¨┬UÂ³\(Ã¹
KÃ¡!" ¶ÂŠÂ¨Ã©Â½└Â‰Â®Â½Ã‹
Ã^Ã¡ÃŽRÃÂ„+TÃ"Ã"WE&[
Â¨→Â>f\)HÃ†nj"Â³S
Â·IÂrÂ¡ Ã·D Ã·\(Ã†┴Â£Â½Ã–
JYfSÃ¤Z├ UÃ¯└Ã'┌ÂÃ«y
Â·Ã"8Ã«YÂ'!* Ã©vÃ"ÂƒÃ™'Â¿mVÂ½Â«FuÂ"Â‹Ã'7Â¯Ã·┤Ã
ÃÃ'ÃžÂ†>]EzÃ–6Â¾Â¿ÂŸÂµÃ^ÂI#ÂŽÃ,Â€TN
Ã«Ã–Ã‹DÂ·ÃthÃÂ«Ã‹Ã¿Ã³Â¡hC8UÂ¶SÃ'7G
┤Â^Ã¡Âœ\)Ã‡Â‡Â½Â°ÂªÃ¨ÃD'!Â™
Â'\n1Q\rÃ¡Ã¸7DBÃ¯:g└Ã^
VÃ†Â'Ã·RÃºÃž◄–Â–Ã®→1☼K}Âe□Â–KÂ…Ã¶ÃšY┤>├

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

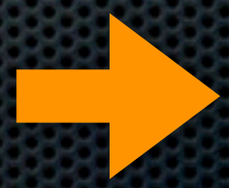
Metagoofil & Linkedin results

- 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.**
Advanced Web Application Defense with ModSecurity — 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

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.

Usercheck.com

USERNAME: laramies CHECK

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
Hellotxt - available	Pownce - available	Yotify - available
Hexday - available	Rejaw - available	Youtube - taken

Using results

- Password profiling

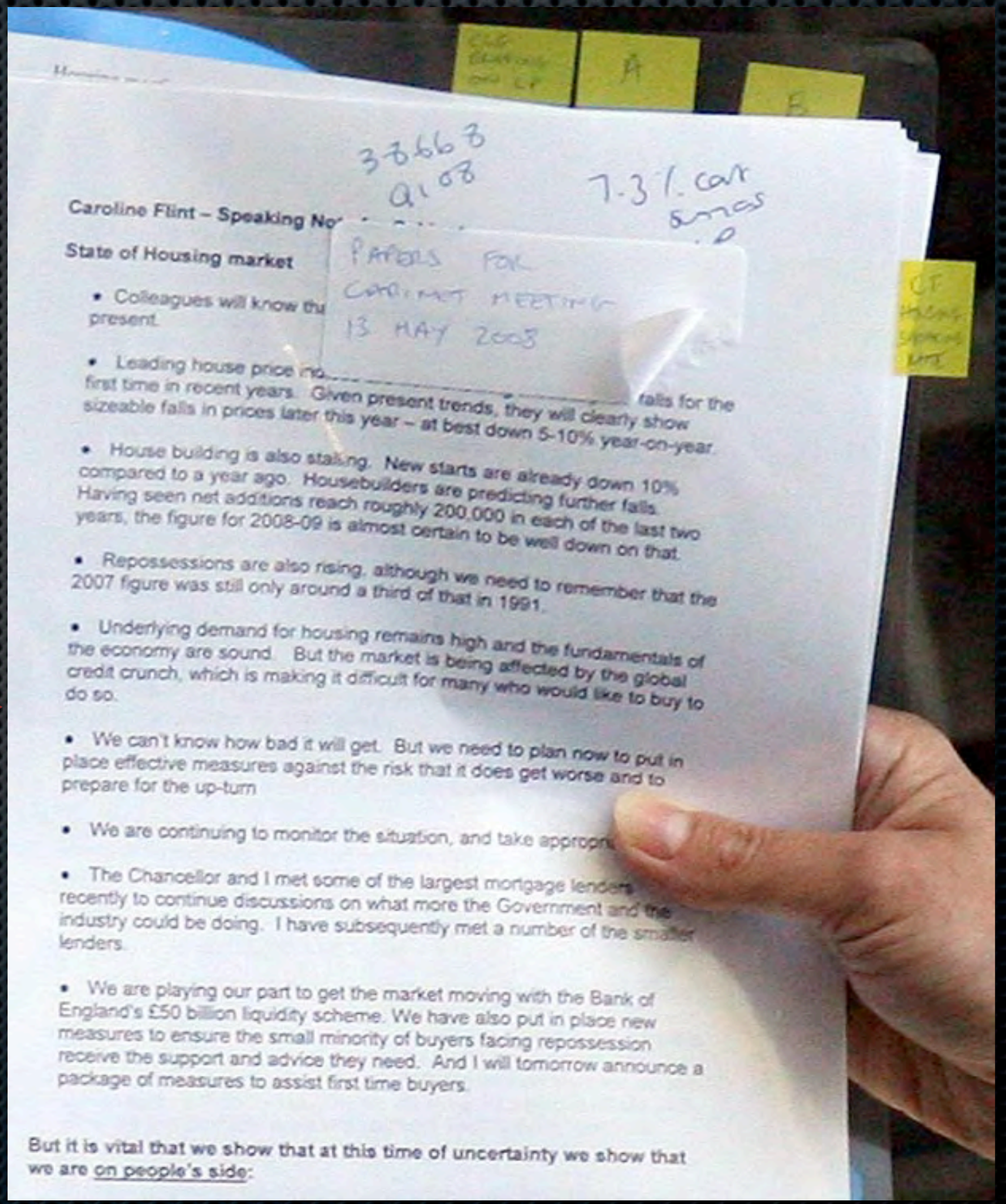
Dictionary creation: words from the different user sites

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

Brute force ATTACK

S21sec
Tomorrow's Digital Security, Today

There are more ways to get info



Caroline Flint – Speaking No

State of Housing market

- Colleagues will know th
present.

- Leading house price in
first time in recent years. Given present trends, they will clearly show falls for the
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 appropri

- 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

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

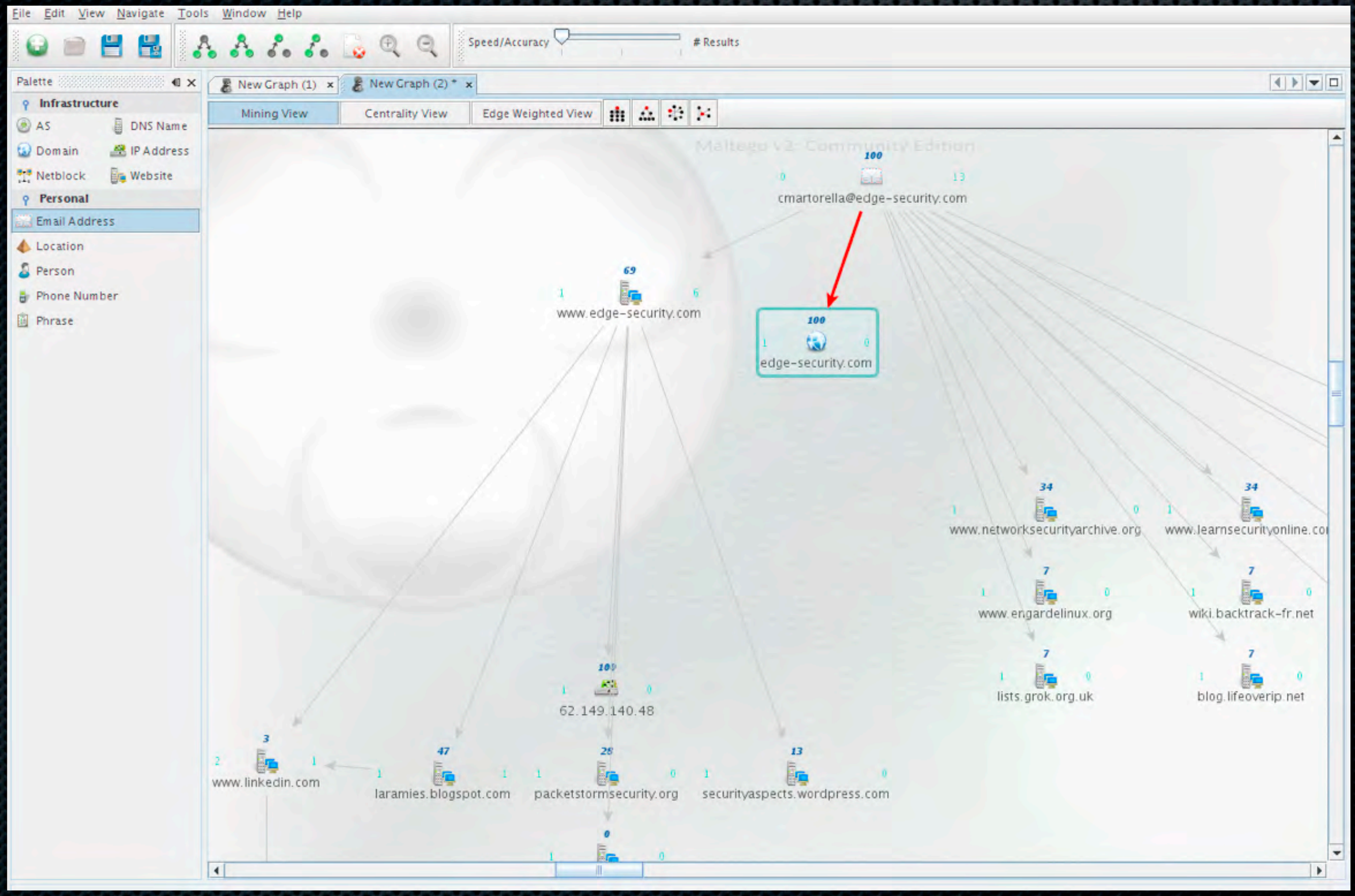
Kyle Doyle's Facebook profile makes it quite obvious he was not off work for a 'valid medical reason'

All together - Maltego

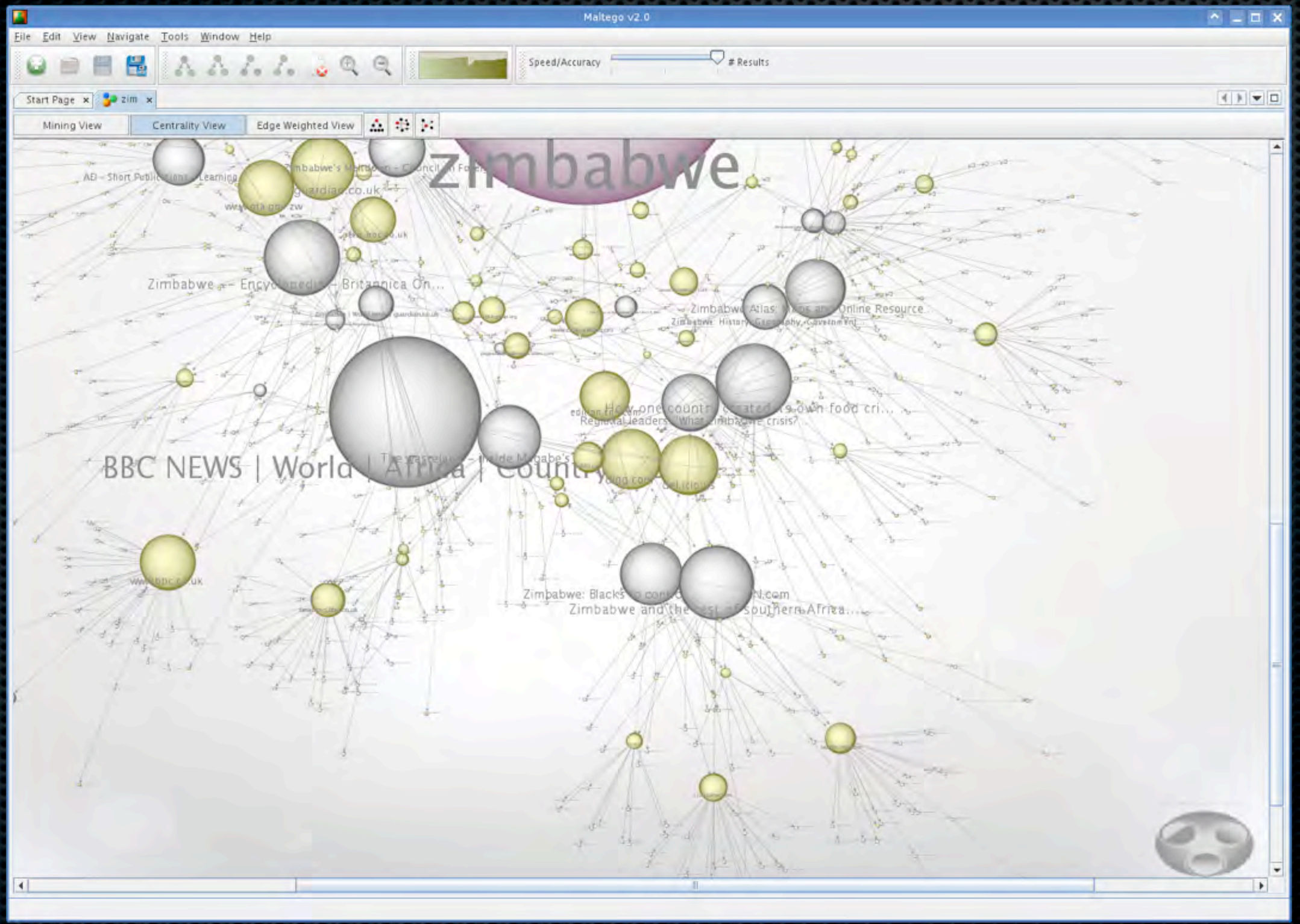
Maltego is “the only” professional Information Gathering tool.

“Information is power
Information is Maltego”

Maltego


File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1)
New Graph (2) *
Mining View
Centrality View
Edge Weighted View
Maltego V2- Community Edition
100
cmartorella@edge-security.com
69
www.edge-security.com
100
edge-security.com
34
www.networksecurityarchive.org
34
www.learnsecurityonline.co
7
www.engardelinux.org
7
wiki.backtrack-fr.net
7
lists.grok.org.uk
7
blog.lifeoverip.net
100
62.149.140.48
3
www.linkedin.com
47
laramies.blogspot.com
25
packetstormsecurity.org
13
securityaspects.wordpress.com
0

Maltego


Maltego v2.0
File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Start Page
zim
Mining View
Centrality View
Edge Weighted View
Zimbabwe
BBC NEWS | World | Africa | Country

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

?

S21sec

Tomorrow's Digital Security, Today

S21sec

Tomorrow's Digital Security, Today

Thank you for coming

cmartorella@s21sec.com
cmartorella@edge-security.com