

Si no quieres que sepa tu nombre,
por que llevas el DNI en la frente?



Christian Martorella
CISSP, CISA

Penetration testing

Information Gathering

Discovery / Fingerprinting

Vulnerability analysis

Exploitation

Reporting

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.

I.G types

Passive

Active

I.G - Types of information

- Domain, subdomain/host names
- User names → jdoe
- **Email Accounts** → **jdoe@target.com**
- **Workers names** → **John Doe**

I.G what for?

- **Host/domain** information for discovering new targets, to get a description of the host, industrial espionage, etc
- **User names, emails, worker names**, for performing brute force attacks on available services.

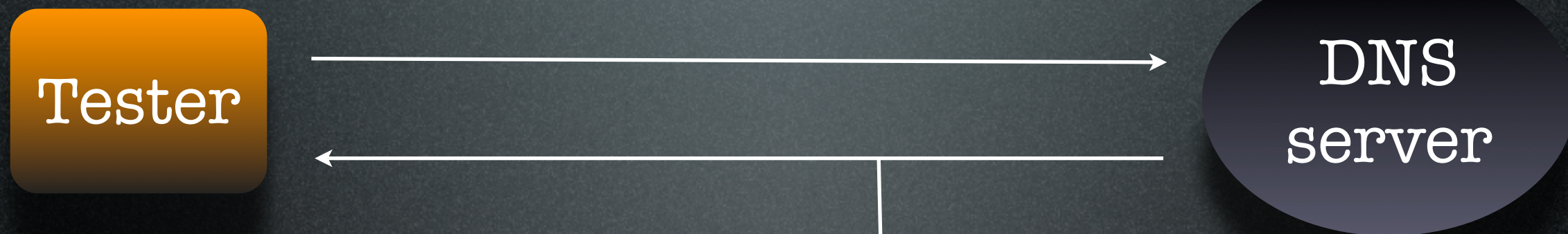
How can we obtain
this kind of info?

Obtaining host and Domains names - Classic

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

Zone-Transfer - DIG

request: `dig @srvr.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



Obtaining host and Domains names II

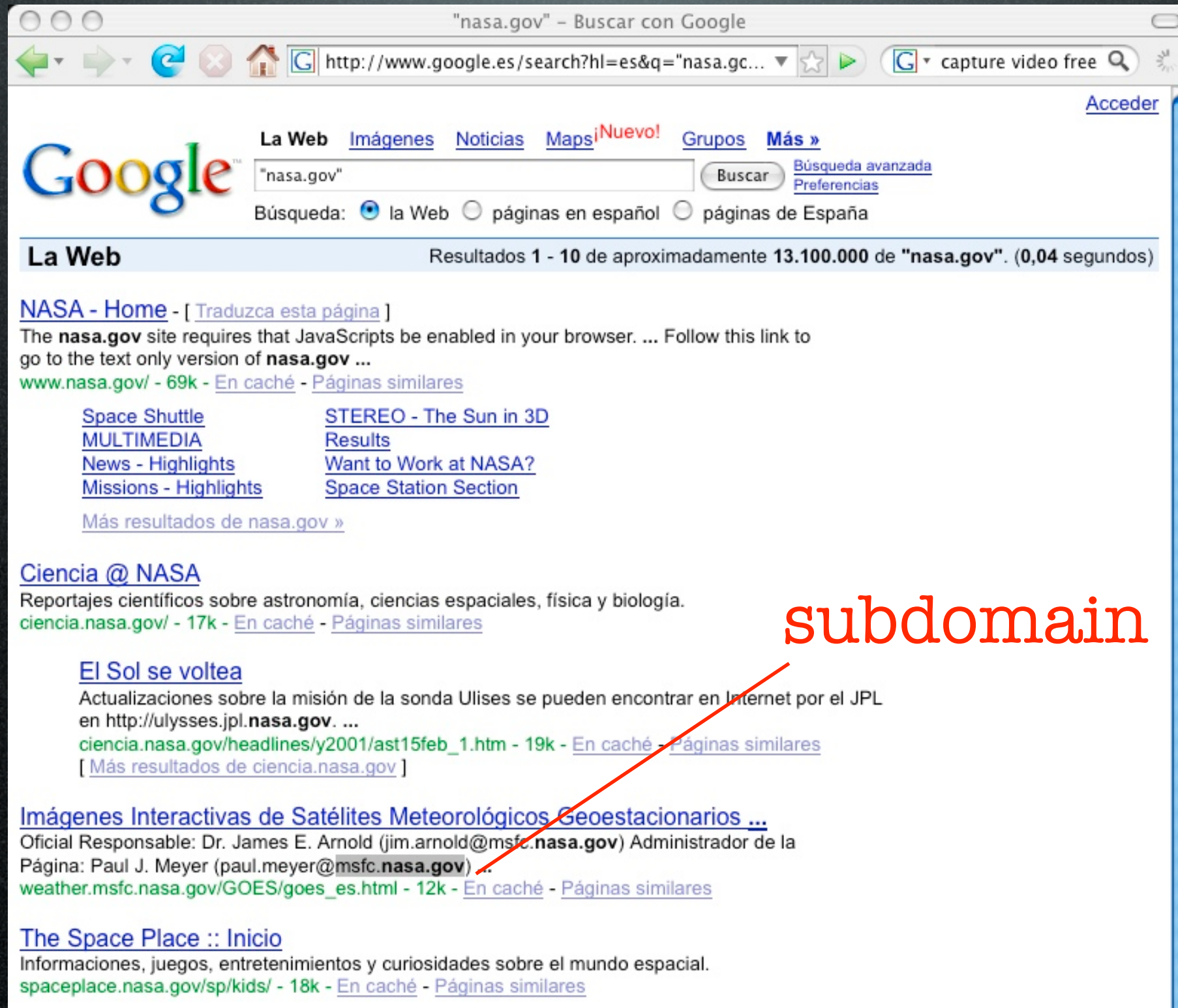
- Search Engines (passive)
- Public PGP key servers (passive)

Obtaining host and Domains names II

- The PGP public key servers are only intended to help the user in exchanging public keys
 - <http://keyserver.veridis.com/>



Obtaining host and Domains - Search engines



The screenshot shows a Google search for "nasa.gov". The search results are categorized under "La Web". The first result is "NASA - Home" with a description: "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 ...". Below this, there are links to "www.nasa.gov/ - 69k", "En caché", and "Páginas similares". There are also links to "Space Shuttle MULTIMEDIA", "News - Highlights", "Missions - Highlights", "STEREO - The Sun in 3D Results", "Want to Work at NASA?", and "Space Station Section". A link to "Más resultados de nasa.gov »" is also present.

The second result is "Ciencia @ NASA" with a description: "Reportajes científicos sobre astronomía, ciencias espaciales, física y biología." Below this, there are links to "ciencia.nasa.gov/ - 17k", "En caché", and "Páginas similares". There is also a link to "El Sol se voltea" with a description: "Actualizaciones sobre la misión de la sonda Ulises se pueden encontrar en Internet por el JPL en http://ulysses.jpl.nasa.gov. ...". Below this, there are links to "ciencia.nasa.gov/headlines/y2001/ast15feb_1.htm - 19k", "En caché", and "Páginas similares". A link to "[Más resultados de ciencia.nasa.gov]" is also present.

The third result is "Imágenes Interactivas de Satélites Meteorológicos Geoestacionarios ..." with a description: "Oficial Responsable: Dr. James E. Arnold (jim.arnold@msfc.nasa.gov) Administrador de la Página: Paul J. Meyer (paul.meyer@msfc.nasa.gov) ...". Below this, there are links to "weather.msfc.nasa.gov/GOES/goes_es.html - 12k", "En caché", and "Páginas similares".

The fourth result is "The Space Place :: Inicio" with a description: "Informaciones, juegos, entretenimientos y curiosidades sobre el mundo espacial." Below this, there are links to "spaceplace.nasa.gov/sp/kids/ - 18k", "En caché", and "Páginas similares".

A red arrow points from the word "subdomain" to the email addresses "jim.arnold@msfc.nasa.gov" and "paul.meyer@msfc.nasa.gov" in the third result, highlighting the "msfc.nasa.gov" part as a subdomain.

Obtaining host and Domain names II



OpenPGP Keyserver - search for keys

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

Page Load Error Page Load Error PGP Corporation - Onl... MIT PGP Key Server OpenPGP Keyserver - ... LinkedIn: Home

KeyServer

@veridis.com

Search

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>	0xF490FA1A	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>	0x472085A4	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.com>	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>	0x1283F49C	2048/1024	1998/11/26	Never
▶ Carlos Espana <cespana@apple.com>	0x2B2E7F4B	2048/1024	2004/06/23	Never
▶ CCS <ccs@asia.apple.com>	0xA45BCE3D	1024	1998/03/17	Never
▶ Chad Lawson <cdlawson@apple.com>	0xF7907FC6	1024/1024	2002/04/11	Never
▶ Chad Williams <chad@apple.com>	0x8830777B	4096/1024	1998/06/05	Never
▶ Charles Vollum <moana@xsw.com>	0x000BFC09	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. Gordon <cagg@interlog.com>	0x7508B6C3	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>	0xBA597DF5	1024	1996/12/17	Never
▶ Chris Jalbert <jalbert@apple.com>	0x802B27EB	2048/1024	1997/09/11	Never
▶ Chris Rives <grampus@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

```
Default
glst.gsfc.nasa.gov ====> 128.183.240.122
isccp.giss.nasa.gov ====> 169.154.204.82
aura.gsfc.nasa.gov ====> 128.183.212.218
www.cdsc.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
lheamail.gsfc.nasa.gov ====> 128.183.16.143
ndrd.gsfc.nasa.gov ====> 128.183.102.200

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

```
gov -l 200 -m google
```

Obtaining user names - Classic

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



Other sources..

Obtaining user names - New sources

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

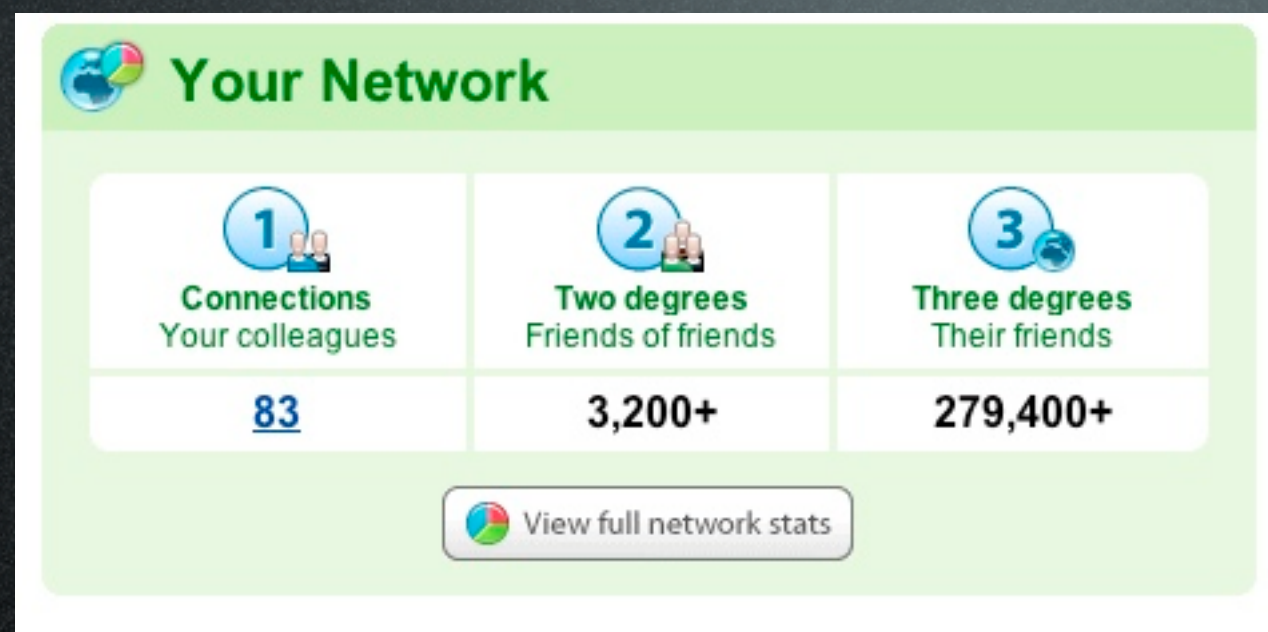
Obtaining user names - New sources

- Social networks



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

Obtaining user names - New sources



Current Job
Pasts Jobs
Education
Job description
Etc...



Social networks, correlations

vizster



zster/images/basic.png

<http://heer.org/vizster/images/basic.png>

Obtaining user names - theHarvester



```
libe libe: Julie Atwood
          Heather Landers
****    Pete Langlois
*The    Megumi Nordby
*Coc    Eric Dawson
*Edg    Tobey Fitch
*cmc    Solomon Eljashev
****    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 Jasinskis
          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.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#
```

Obtaining user names - New sources

Metadata: is data about data.

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

Obtaining user names - 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



logo-Ubuntu.png



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



logo-Kubuntu.png



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

:/

Metadata

- So where can we get interesting metadata?



Metadata

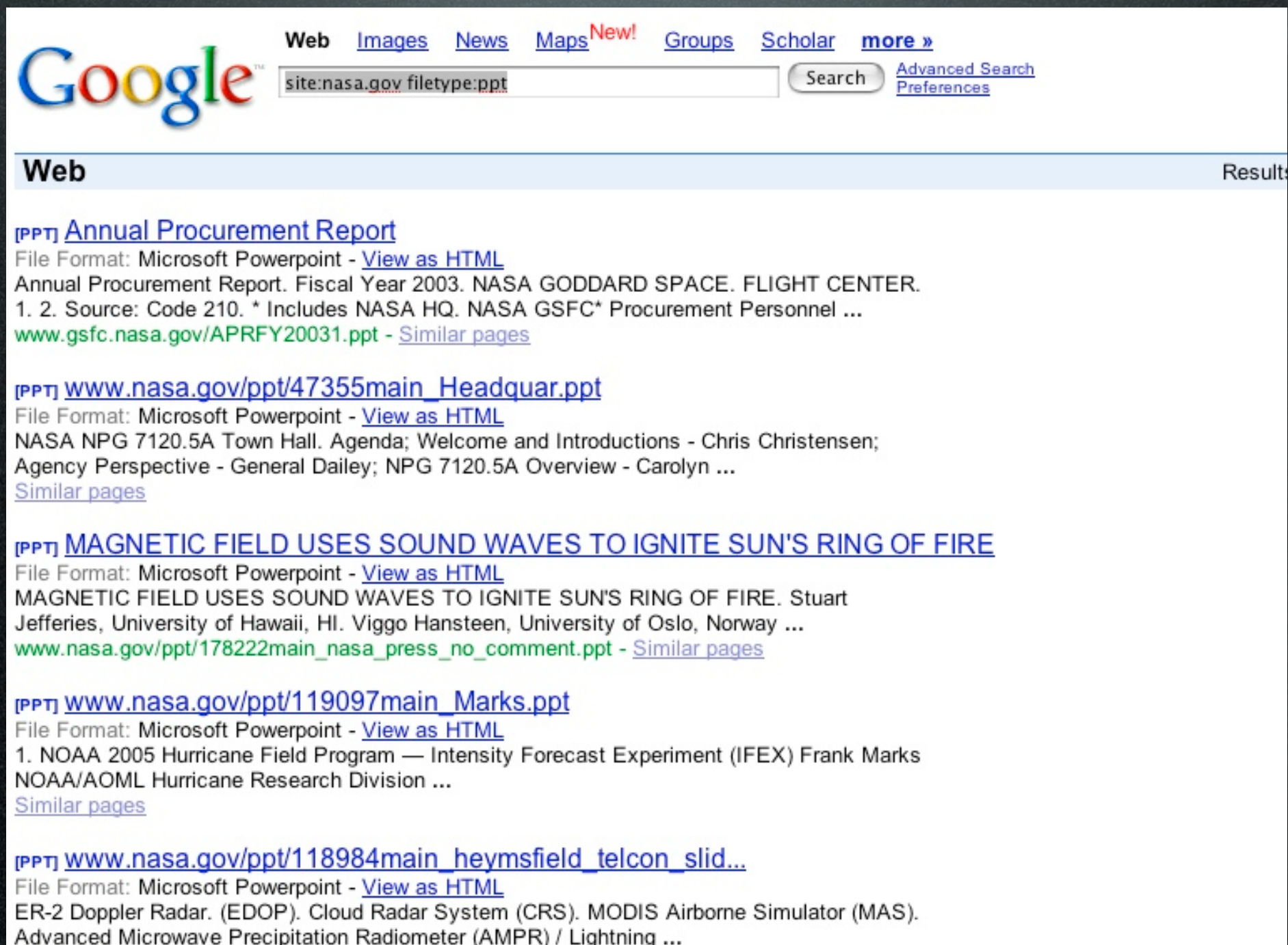
- Ok, I understand metadata... so what?

Metagoo^{oo}fil

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

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 includes a link to 'View as HTML'. The second result is titled '[PPT] www.nasa.gov/ppt/47355main_Headquar.ppt' and also includes a 'View as HTML' link. The third result is titled '[PPT] MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE' and includes a 'View as HTML' link. The fourth result is titled '[PPT] www.nasa.gov/ppt/119097main_Marks.ppt' and includes a 'View as HTML' link. The fifth result is titled '[PPT] www.nasa.gov/ppt/118984main_heymsfield_telcon_slid...' and includes a 'View as HTML' link. Each result also provides a brief description of the content and a link to 'Similar pages'.

Google 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](#)

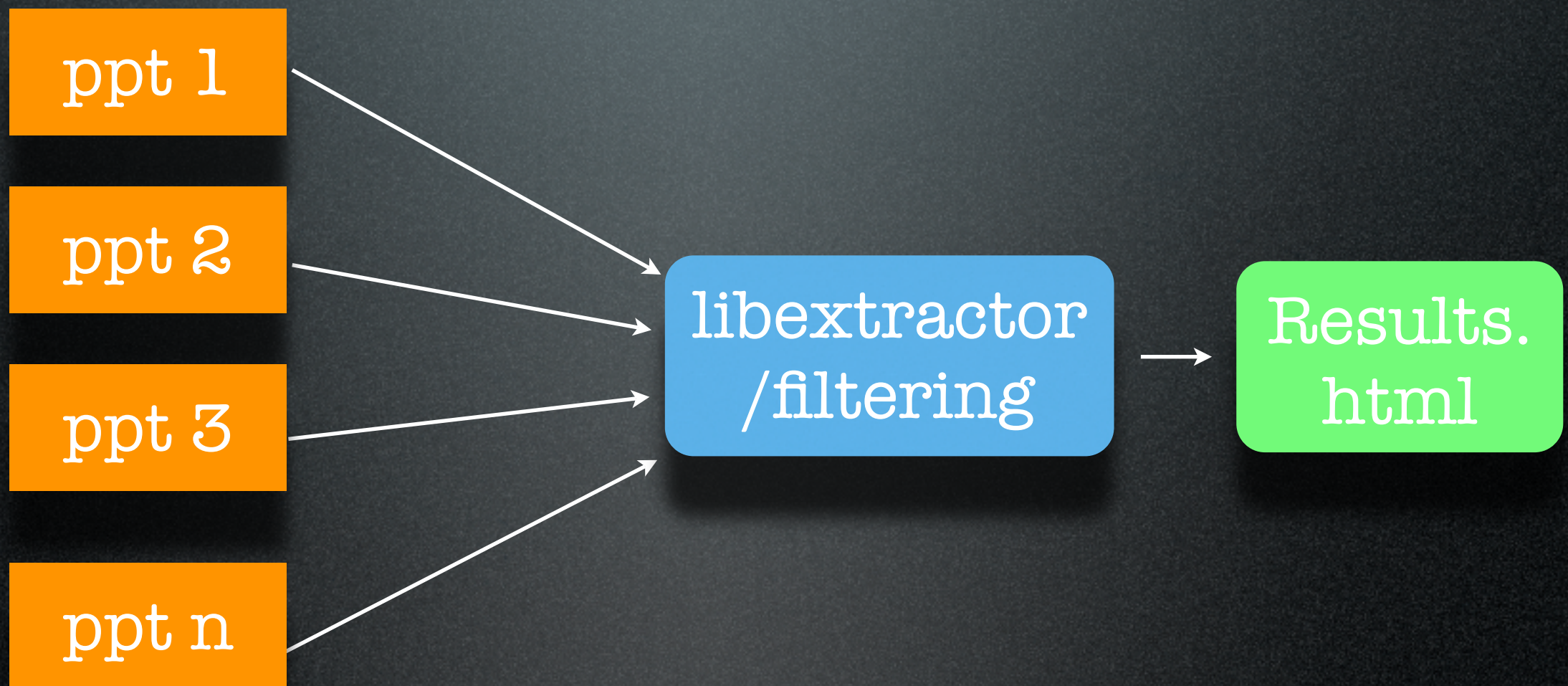
[\[PPT\] MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE](#)
File Format: Microsoft Powerpoint - [View as HTML](#)
MAGNETIC FIELD USES SOUND WAVES TO IGNITE SUN'S RING OF FIRE. Stuart
Jefferies, University of Hawaii, HI. Viggo Hansteen, University of Oslo, Norway ...
[www.nasa.gov/ppt/178222main_nasa_press_no_comment.ppt](#)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

Metagoo^{fil}

Downloaded files



Metagoofil

```
laramies@salvation: ~/edgesec/metagoofil
File Edit View Terminal Tabs Help
laramies@salvation: ~/edgesec/metagoofil x laramies@salvation: ~/edgesec/metagoofil x
laramies@salvation:~/edgesec/metagoofil$ python metagoofil.py

*****
*MetaGooFil Ver. 1.2d          *
*Coded by Christian Martorella *
*Edge-Security Research       *
*cmartorella@edge-security.com *
*****

MetaGooFil 1.2

usage: metagoofil options

    -d: domain to search
    -f: filetype to download (all,pdf,doc,xls,ppt, etc)
    -l: limit of results to work with (default 100)
    -o: output file, html format.
    -t: target directory to download files.

    Example: metagoofil.py -d microsoft.com -l 20 -f all -o micro.html -t micro
o-files

laramies@salvation:~/edgesec/metagoofil$
```

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/IMDCPrewrite.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_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.
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\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:\
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's Docs:* Peter's Data* :* GSFC R&TD *:FY07 R&TD Planning:FY07 IntegInve
C:\WINDOWS\Desktop\
```

Metagoofil - results

Total authors found (potential users):

```
RÄYÄÄÄÄ9RÄ|8\|nÄ"UÄ³\(\Ä¹
KÄi!" ¶ÄŠÄ"Ä©Ä½¹Ä¾Ä©Ä½Ä,
Ä"ÄiÄžRÄÄ,,+TÄ"Ä"WE&[
Ä"-Ä>f\|HÄ+nj"Ä³S
Ä·IÄrÄi8Ä·D      Ä·\(\Ä+¹Ä£Ä½Ä-
Ä-ÄµÄ,,ÄŠ|1ÄµÄ¹Ä°`      Ä·ÄjÄ
Ä½]3ÄÄ,,\n8Ä...ÄŠHÄ¾_xÄ';
  Ä-Ä-XÄ,Ä'=vÄ|¹!!Ä"Ä¾Ä+Ä¿8
JYfSÄ²Z| UÄ¹¹Ä'¹ÄÄy
Ä·Ä"8Ä«YÄ'!*  Ä©vÄ"ÄfÄ™¹Ä¿mVÄ½Ä«FuÄ"Ä¹Ä'7Ä-Ä·¹Ä
ÄÄ'ÄžÄ+>]EzÄ-6Ä¾Ä¿ÄÝÄµÄ¹ÄI#ÄžÄ,Ä€TN
Ä«Ä-Ä¹DÄ·ÄthÄÄ«Ä¹Ä¿Ä³Ä¹hC8UÄ¹SÄ'7G
¹Ä¹Ä¹Äæ\|Ä+Ä+Ä¾Ä°Ä«Ä¹ÄD'¹Ä™
  Ä'\n1Q\rÄiÄ,7DBÄ¹:g¹Ä¹
VÄ¹Ä¹Ä·RÄ°ÄžÄ-Ä-Ä®¹¹K}ÄeÄÄ-KÄ...Ä¹ÄšY|>|
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
```

Metagoofil & Linkedin results

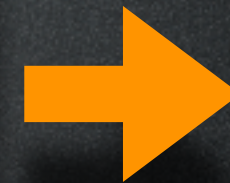
- Now we have a lot of usernames, what can i do?

Using results

- User profiling
- Dictionary creation John Doe



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



ATTACK!

References

- www.edge-security.com
- blog.s21sec.com
- www.s21sec.com
- www.gnunet.org/libextractor/
- www.linkedin.com

Any question ?



Tomorrow's Digital Security, Today

Thank you for coming