Is here again….

Chema Alonso

Informática 64

www.informatica64.com

Previously on FOCA…..

FOCA 0.X

MetaExtractor

Archivo Pestañas Metadatos Opciones Sobre...

Windows 7 + Serve... | Diez_errores_que_... | 03texas.xls | 04tbl59a.xls | w99tbl01.xls

Codificación: Latin I
Autor: Gonzalo
Plantilla: Normal
Última vez guardado por: Chema
Revisión: 8
Aplicación: Microsoft Office Word
Tiempo de edición: 00:38:00
Fecha de creación: 11/10/2009 10:54:00
Última vez guardado: 13/10/2009 11:42:00
Páginas: 2
Palabras: 682
Carácteres: 3757
Compañia: Neurocrypt
Lineas: 31
Parrafos: 8
SO: Windows 7

What kind of data can be found?

- Metadata:
  - Information stored to give information about the document.
    - For example: Creator, Organization, etc..
- Hidden information:
  - Information internally stored by programs and not editable.
    - For example: Template paths, Printers, db structure, etc…
- Lost data:
  - Information which is in documents due to human mistakes or negligence, because it was not intended to be there.
    - For example: Links to internal servers, data hidden by format, etc…

Metadata Risks

- "Secret" relationships
  - Government & companies
  - Companies & providers
- Piracy
- Reputation
- Social engineering attacks
- Targeting Malware

2003 – MS Word bytes Tony Blair

Microsoft Word bytes Tony Blair in the butt

Home > Privacy > **Blair's Iraq Dossier**

Richard M. Smith (rms@computerbytesman.com)
June 30, 2003

Microsoft Word documents are notorious for containing private information in file headers which people would sometimes rather not share. The l
hard way.

Back in February 2003, 10 Downing Street published a dossier on Iraq's security and intelligence organizations. This dossier was cited by Colin
Dr. Glen Rangwala, a lecturer in politics at Cambridge University, quickly discovered that much of the material in the dossier was actually plagiar

You can read Dr. Rangwala's original analysis of the dossier from Feb. 5, 2003 at this URL:

http://www.casi.org.uk/discuss/2003/msg00457.html

Blair's government made one additional mistake: they published the dossier as a Microsoft Word file on their Web site. When I first heard from I
had worked on the document. I downloaded the Word file containing the dossier from the 10 Downing Street Web site (http://www.number-10.

```
Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"
```

Targeting Malware

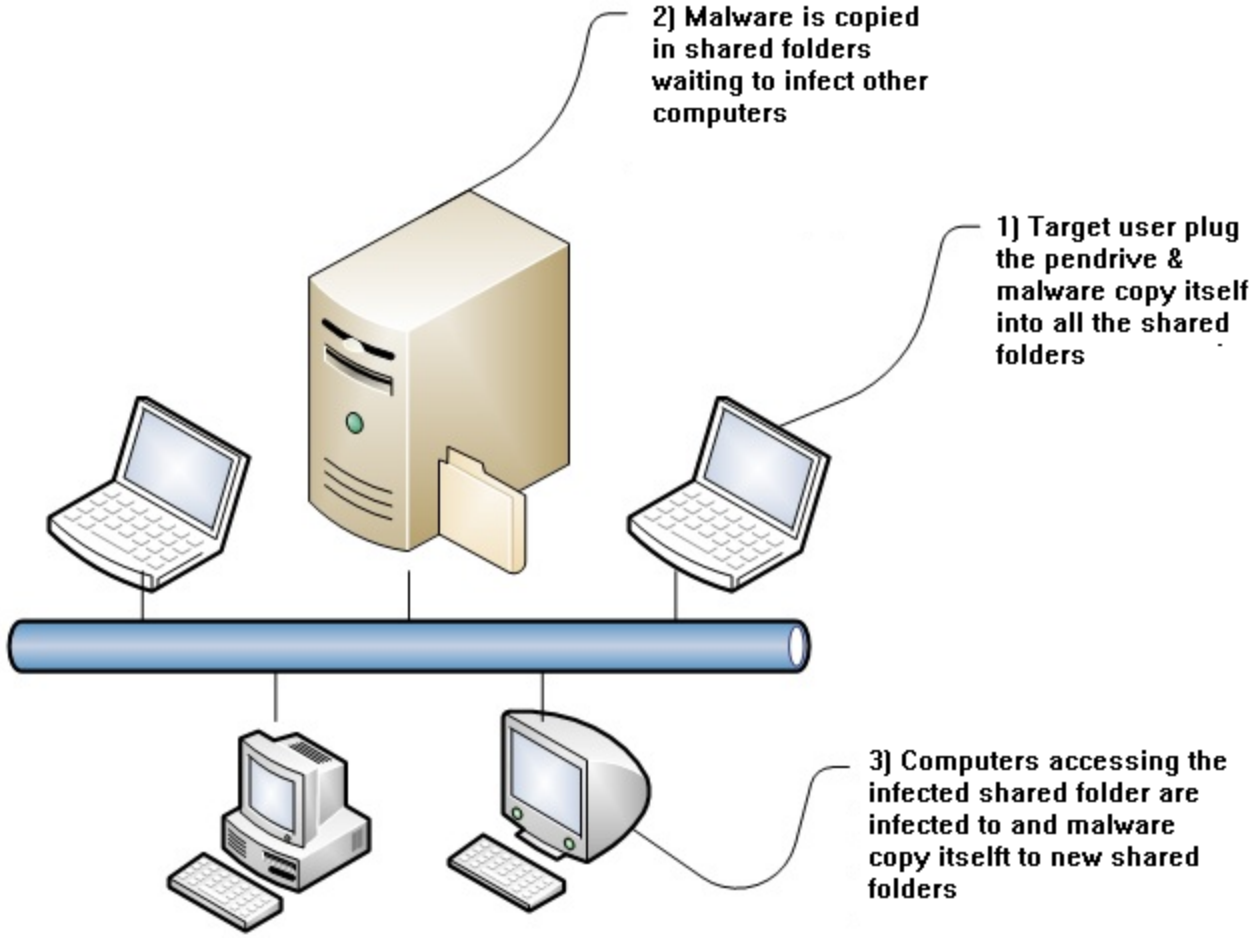
Pentagon breached by foreign hacker

A foreign spy agency carried out the most serious "cyber attack" on the US military's networks when a tainted flash drive was inserted into a laptop in the Middle East, according to a senior Pentagon official.

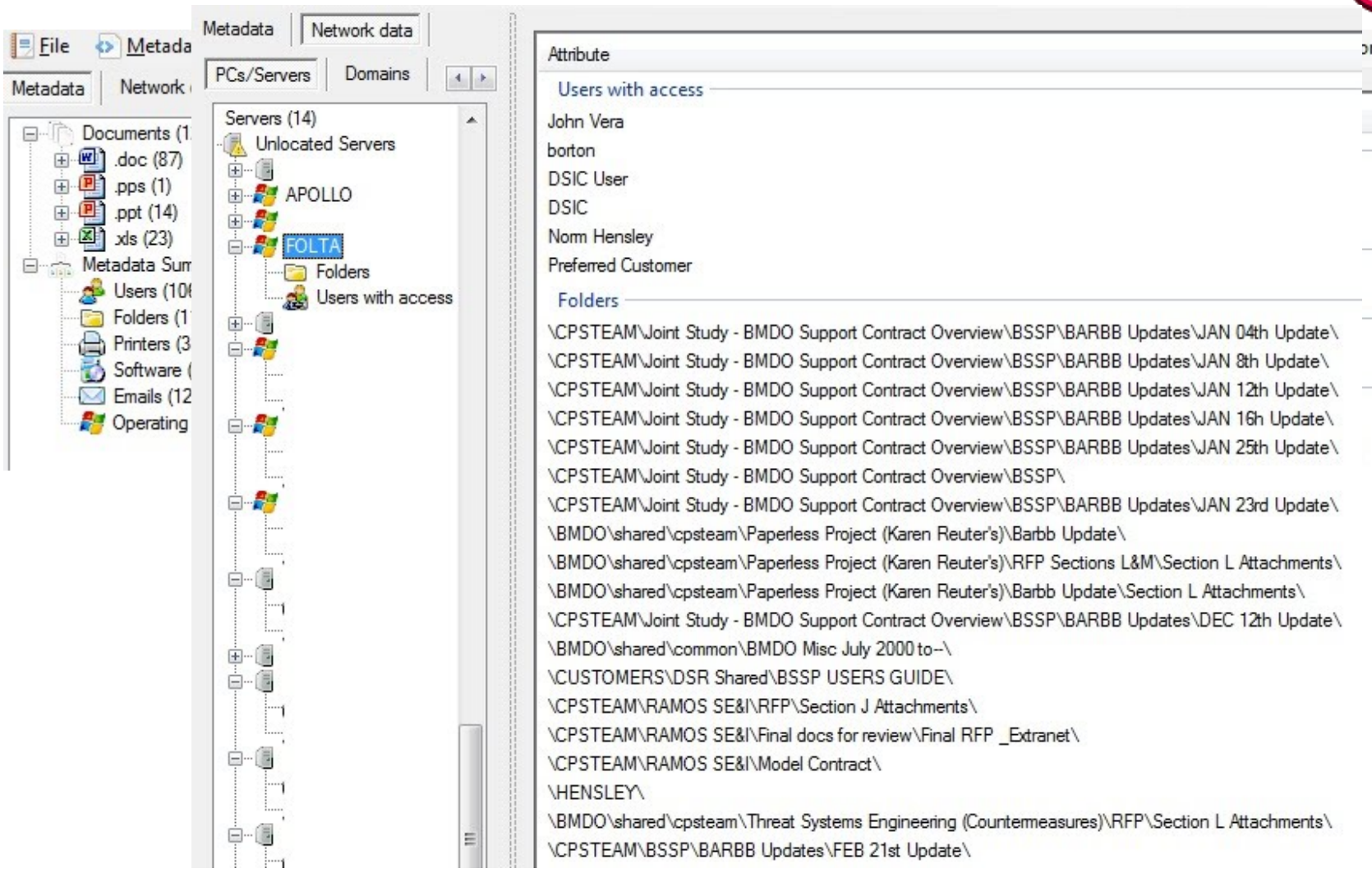
By Alex Spillius, Washington
Published: 9:43PM BST 26 Aug 2010

The Pentagon faces regular cyber attacks Photo: GETTY

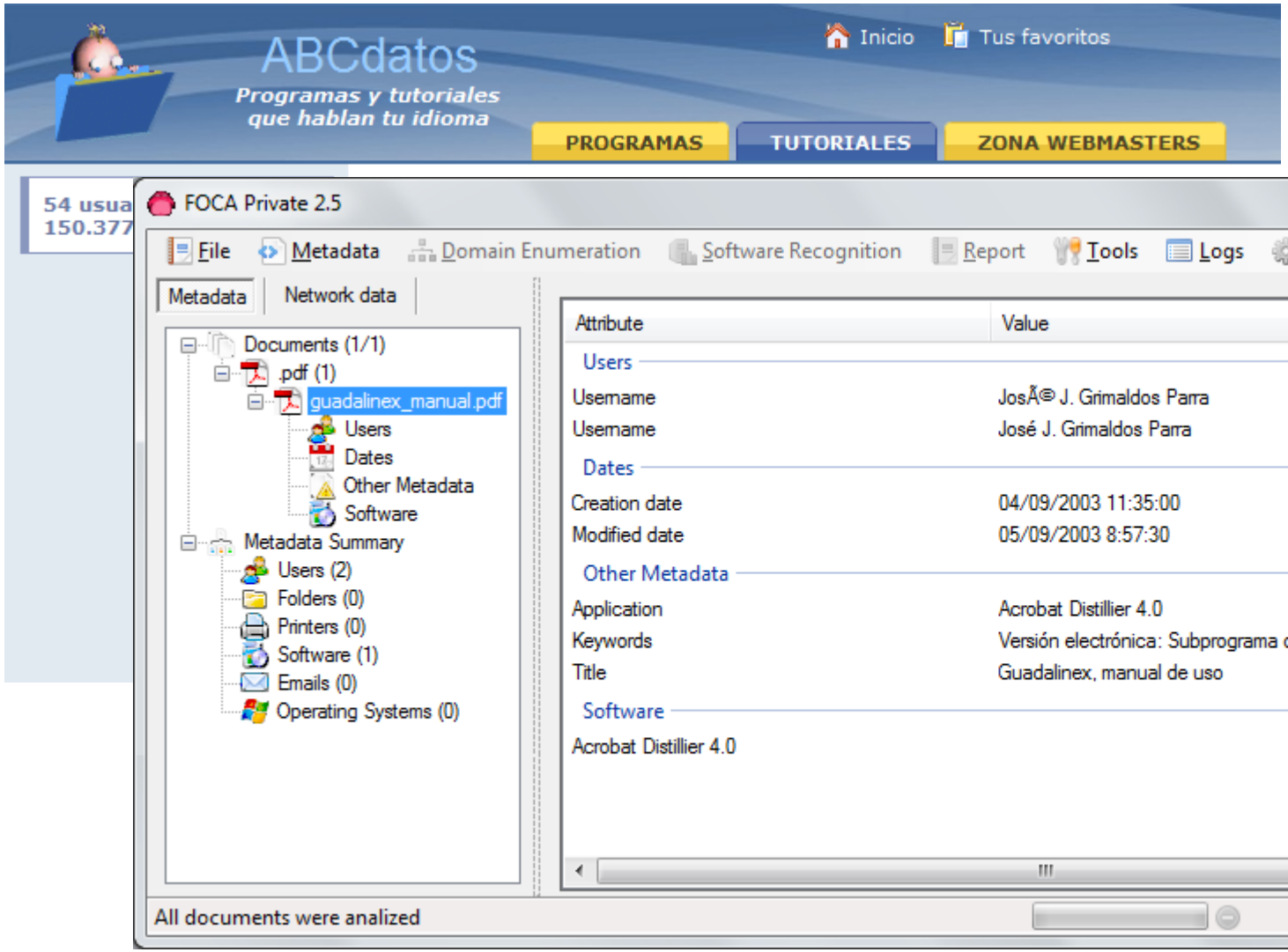
Targeting Malware



Electing the entry point



Social Engineering Attack



Anonym0us case

thinq_ Search

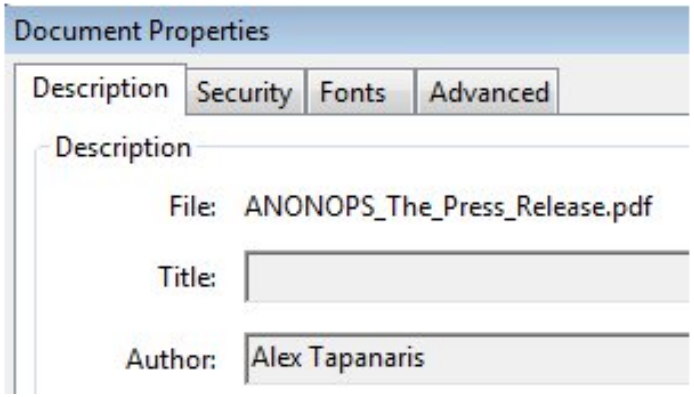
Designer arrested over Anonymous press release

Nabbed by the properties

Written by Paul Hales on *15 December, 2010* NEWS > WEB

A bloke named Alex Tapanaris, whose name appeared on the PDF press release circulated by online trouble-makers Anonymous has had his web site disappeared from the web and, according to a post on pastebin.com, the unfortunate chap has been arrested.

The release was circulated last Friday and pretty soon the document's properties were noticed.



Spookily on Monday, Tapanaris' web site

GPS information

EXIF data

Exif Version	0221
Color Space	1
Pixel Y Dimension	0
Date Time Original	2011:02:08 20:23:15
Date Time Digitized	2011:02:08 20:23:15
Exposure Time	1/10
F Number	2.8
Exposure Program	Normal program
ISO Speed Ratings	1000
Shutter Speed Value	3.3242976835879743
Aperture Value	2.970853573907009
Metering Mode	Average
Flash	No flash function
Subject Area	[4 values]
Focal Length	3.85
Sensing Method	One-chip color area sensor
White Balance	Auto white balance
Make	Apple
Model	iPhone 3GS

Tweet 0 Tykkää Configure Close

Lost Data

Penetration Tester's Open Source Toolkit: 2
by Chris Hurley

32 us

View: Front Cover | Table of Contents | Copyright | Excerpt | Index

Previous Page | Zoom in | Next Page

Copyrighted Material

Elsevier, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Elsevier, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Elsevier, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BAL923457U
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

FOCA: File types supported

- Office documents:
  - Open Office documents.
  - MS Office documents.
  - PDF Documents.
    - XMP.
  - EPS Documents.
  - Graphic documents.
    - EXIFF.
    - XMP.
  - Adobe Indesign, SVG, SVGZ (NEW)

What can be found?

- Users:
  - Creators.
  - Modifiers .
  - Users in paths.
    - C:\Documents and settings\jfoo \myfile
    - /home/johnnyf
- Operating systems.
- Printers.
  - Local and remote.
- Paths.
  - Local and remote.
- Network info.
  - Shared Printers.
  - Shared Folders.
  - ACLS.
- Internal Servers.
  - NetBIOS Name.
  - Domain Name.
  - IP Address.
- Database structures.
  - Table names.
  - Colum names.
- Devices info.
  - Mobiles.
  - Photo cameras.
- Private Info.
  - Personal data.
- History of use.
- Software versions.

Demo:
Single files

Sample: FBI.gov

Google site:fbi.gov filetype:xls Buscar Búsqueda avanzada Preferencias

Buscar en: la Web páginas en español páginas de España

La Web Resultados **1** - **10** de aproximadamente **2.190** de **filetype:xls** en el dominio **fbi.gov** (**0,16** segundos)

Google site:fbi.gov filetype:doc Buscar Búsqueda avanzada Preferencias

Buscar en: la Web páginas en español páginas de España

La Web Resultados **1** - **10** de aproximadamente **161** de **filetype:doc** en el dominio **fbi.gov** (**0,15** segundos)

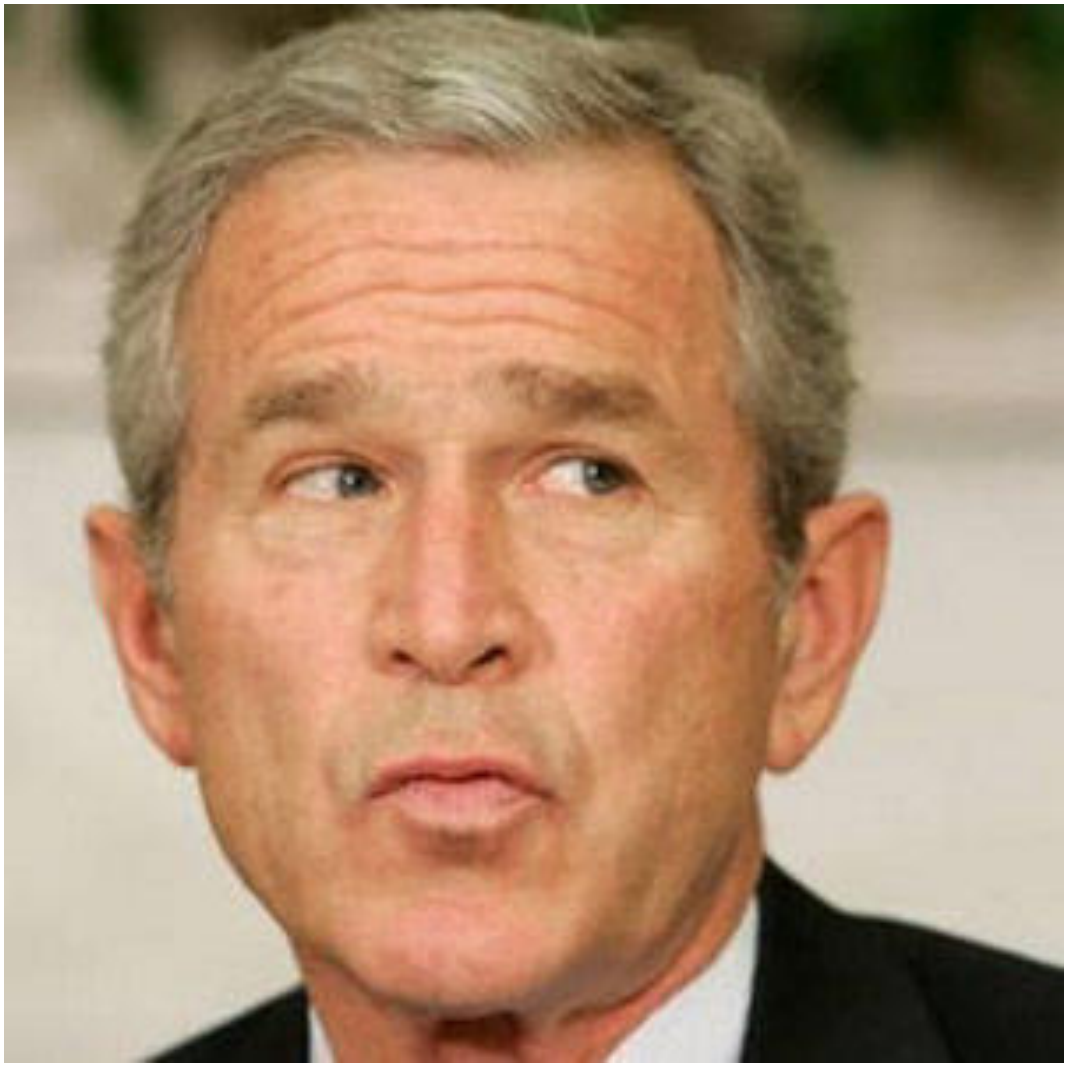
Google site:fbi.gov filetype:pdf Buscar Búsqueda avanzada Preferencias

Buscar en: la Web páginas en español páginas de España

La Web Resultados **1** - **10** de aproximadamente **2.490** de **filetype:pdf** en el dominio **fbi.gov** (**0,17** segundos)

Total: 4841 files

Are they cleaned?



Metadata in Search Engines

Google

site:fbi.gov intitle:"Documents" filetype:pdf Buscar

Buscar en: la Web páginas en español páginas de Espa

a Web

[PDF] C:\Documents and Settings\mdrewniak\Local Settings\Temporary ... - [Trad
rmato de archivo: PDF/Adobe Acrobat - Versión en HTML
ited States Department of Justice. U.S. Attorney, District of New Jersey. 970 Broad Street,
eventh Floor. Newark, New Jersey 07102 ...
wark.fbi.gov/dojpressrel/2008/nk112408.pdf - Páginas similares

:\Documents and Settings\TCalloway\Local Settings\Temporary ... - [Traducir e
embers of the public are reminded that the indictment contains only charges. A defendant is
esumed innocent of the charges and it will be the ...
obile.fbi.gov/dojpressrel/pressrel08/onlineextortion100108.pdf - Páginas similares

[PDF] C:\Documents and Settings\dwashington\Local Settings\Temporary ... - [Tra
rmato de archivo: PDF/Adobe Acrobat - Versión en HTML
ited States Attorney. Southern District of New York. FOR IMMEDIATE RELEASE CONTACT
S. ATTORNEY'S OFFICE. APRIL 20, 2004. MARVIN SMILON, HERBERT HADAD ...
ww.fbi.gov/dojpressrel/pressrel04/drywall.pdf - Páginas similares

[PDF] C:\Documents and Settings\usagan-mmorgan\Desktop\PRESS RELEASE
rmato de archivo: PDF/Adobe Acrobat - Versión en HTML
ited States Attorney David E. Nahmias. Northern District of Georgia. FOR IMMEDIATE
ELEASE. CONTACT: Patrick Crosby. 06/19/08. (404)581-6016

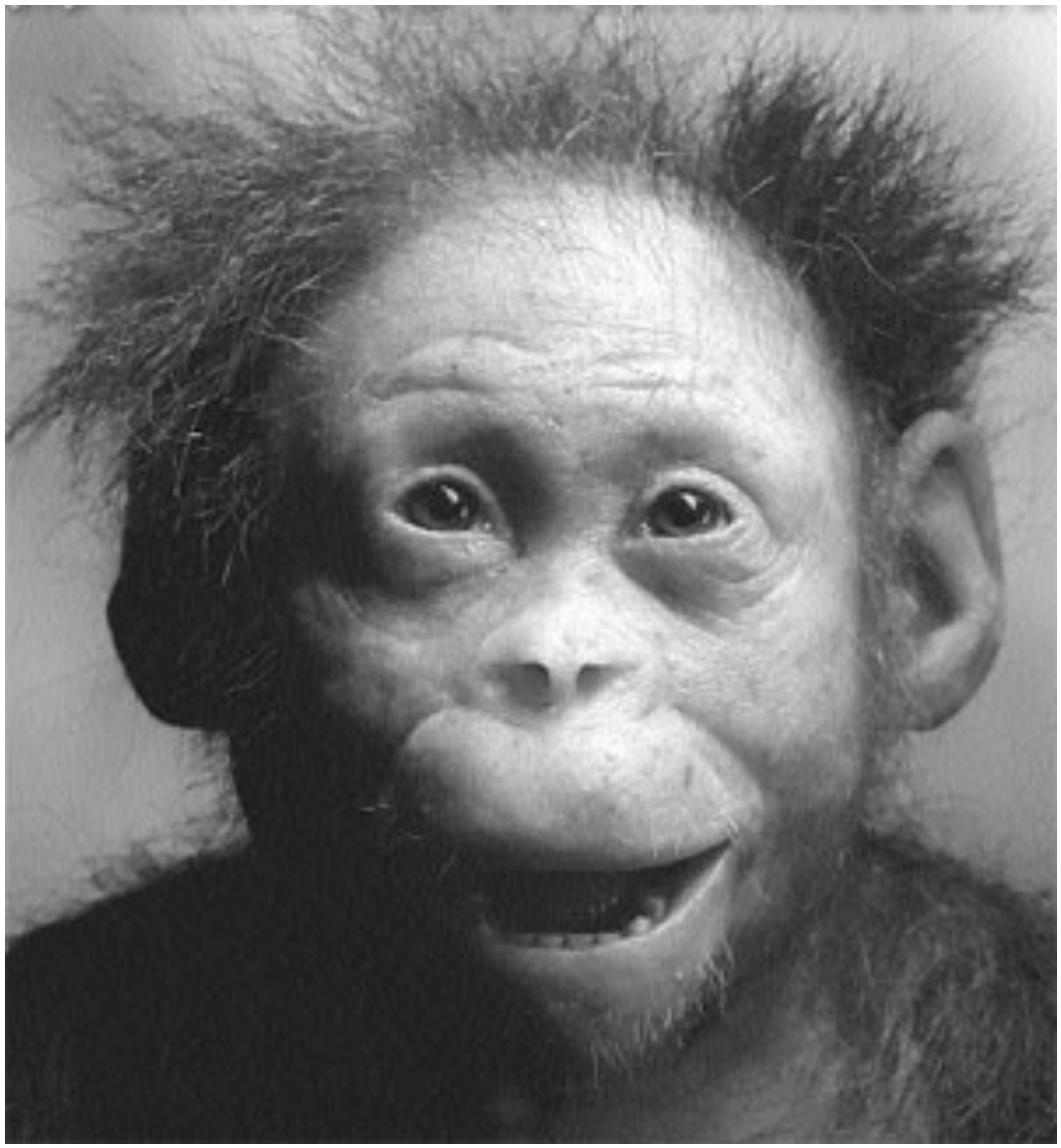
FOCA 1 v. RC3

- Fingerprinting Organizations with Collected Archives
  - Search for documents in Google and Bing
  - Automatic file downloading
  - Capable of extracting Metadata, hidden info and lost data
  - Cluster information
  - Analyzes the info to fingerprint the network.

Demo:

A lot of files

How may days to do the pentesting?



Sometimes don´t

US Army Corps of Engineers
Mobile District
Engineering Division

Warning! **The following unsecured FTP site is for temporary uploading and downloading of files for official government use only. Any other use is unauthorized. Use of this unsecured FTP site is at your own risk.**

The U.S. Army Corps of Engineers, Mobile District, does not exercise any editorial control over the files and information you may find at this location.

ftp://ftp.sam.usace.army.mil/

http://www.sam.usace.army.mil/en/Upload/FTPLink.html

FOCA 2.5

- Network Discovery
- Recursive algorithm
- Information Gathering
- Sw Recognition
- DNS Cache Snooping
- Reporting Tool

DNS Search Panel

Select search type

- Web Searcher
- DNS Search
- Transfer Zone
- Names Search
- Google Sets
- IP Bing
- PTR Scanning

Search IP in Bing

Bing allows search links located in a particular IP address.
This funcionalitty can be used to find domains that
share IP Address.

Select the web search engine to use:

BingWeb

Bing Web limitations

-Max 1000 results for each search

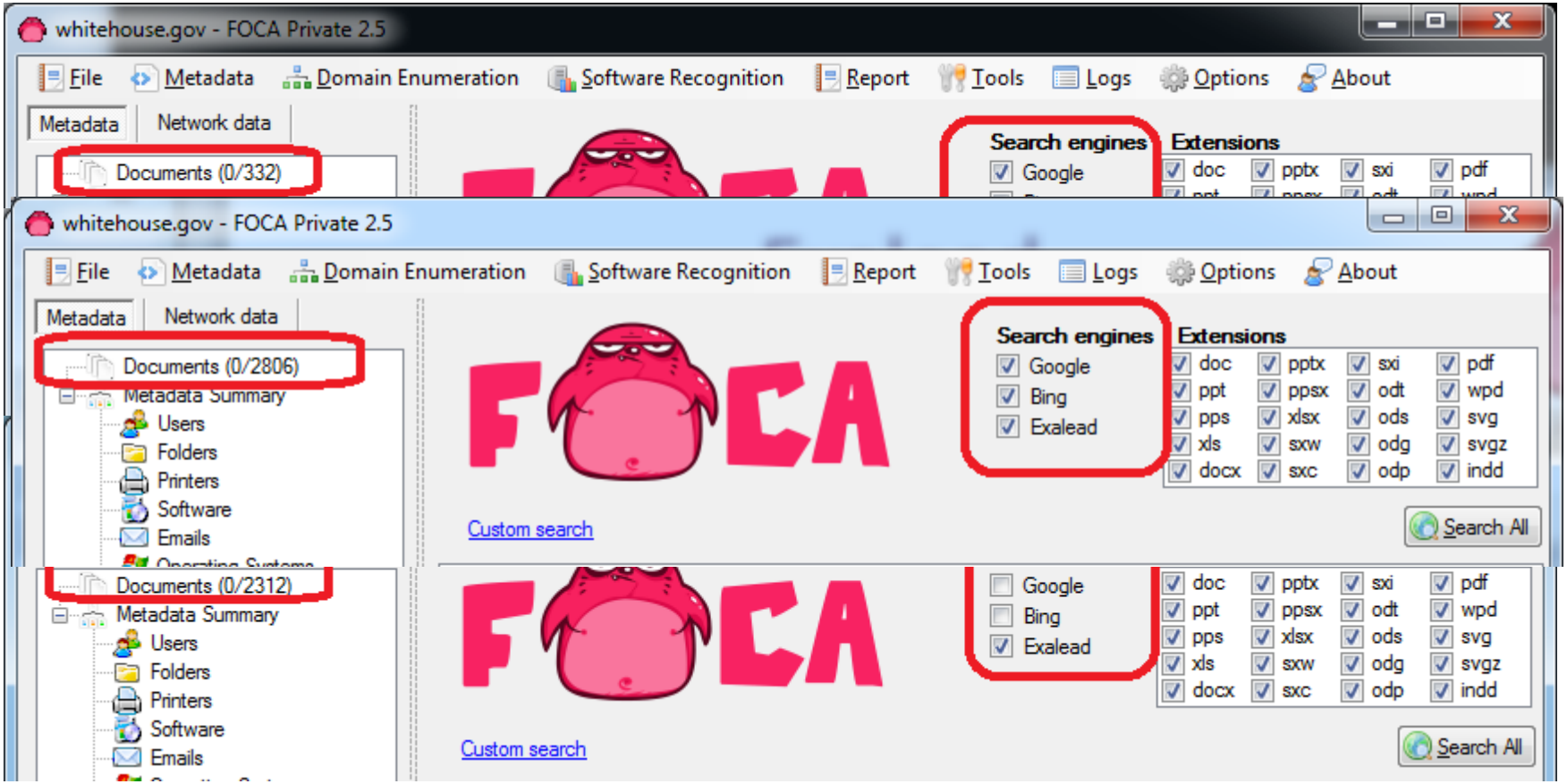
-Max 49 words in a search string

Current search: None

Skip

Start

FOCA 2.5: Exalead



Huge domains case

Google

site:army.mil Buscar

Technology recognition | Crawling | Exploiting | Search | Log

regjeringen.no - FOCA Pro 2.6

File | Metadata | Domain Enumeration | Software Recognition | Report | Tools | Logs | Options | About

Network data | Metadata

PCs/Servers | Domains | IPs | Roles | Vulnerabilities

- regjeringen.no
  - Clients (0)
  - Servers (3)
    - 79.0.0.0
      - 79.171.0.0
        - 79.171.83.0
          - fremtidenshelsetjeneste
    - 81.0.0.0
      - 81.93.0.0
        - 81.93.171.0
          - beta.regjeringen.no [81
    - 195.225.28.0
      - regjeringen.no [195.225.28.19
    - Unlocated Servers

Attribute	Value
Information	
Name	fremtidenshelsetjeneste.regjeringen.no [79.171.83.180]
Domains - Source	
fremtidenshelsetjeneste.regjeringen.no	WebSearch, BingAPI [fremtidenshelsetjeneste.regjeringen.no]
IP Addresses - Source	

Technology recognition | Crawling | Exploiting | Files | Log

Minimize

Google Bing Exalead

doc xls ppsx sxc ods pdf svgz
ppt docx xlsx sxi odg wpd indd
pps pptx sxw odt odp svg

All None

Searching

Stop

Domain: fremtidenshelsetjeneste.regjeringen.no

Files (0 found) | Folders (1 found) | Documents published (0 found) | Backups (0 found)

Directory Listing enabled (0 found) [PASIVE] | Methods on folders (0 found) [PASIVE]

Document

Searching subdomains of regjeringen.no in BingAPI

DNS Search & Zone Transfer

- IP resolution
- Well-Known records
  - NS
  - TXT (SPF)
  - MX
  - SOA (Primary.master)
- Zone Transfer
- Diccionary search

Network Discovery Algorithm

http://apple1.sub.domain.com/~chema/dir/fil.doc

1) http -> Web server
2) GET Banner HTTP
3) domain.com is a domain
4) Search NS, MX, SPF records for domain.com
5) sub.domain.com is a subdomain
6) Search NS, MX, SPF records for sub.domain.com
7) Try all the non verified servers on all new domains
    1) server01.domain.com
    2) server01.sub.domain.com
8) Apple1.sub.domain.com is a hostname
9) Try DNS Prediction (apple1) on all domains
10) Try Google Sets(apple1) on all domains

Network Discovery Algorithm

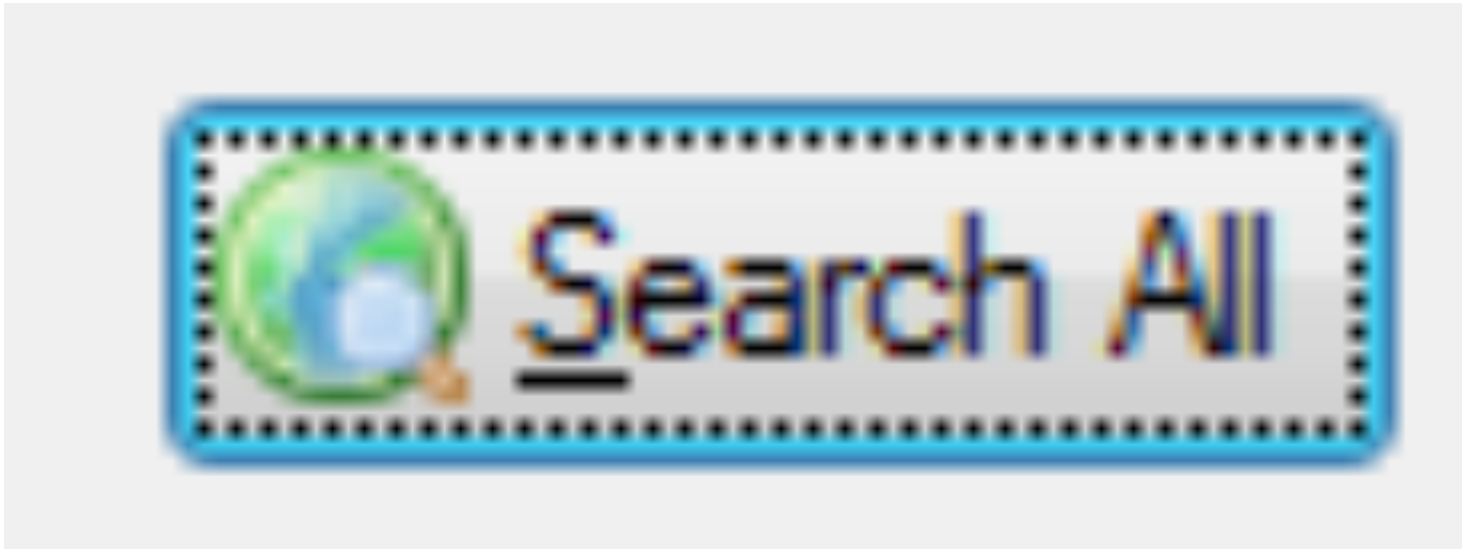
http://apple1.sub.domain.com/~chema/dir/fil.doc

11) Resolve IP Address
12) Get Certificate in https://IP
13) Search for domain names in it
14) Get HTTP Banner of http://IP
15) Use Bing Ip:IP to find all domains sharing it
16) Repeat for every new domain
17) Connect to the internal NS (1 or all)
18) Perform a PTR Scan searching for internal servers
19) For every new IP discovered try Bing IP recursively
20) ~chema -> chema is probably a user

Network Discovery Algorithm

http://apple1.sub.domain.com/~chema/dir/fil.doc

21) / , /~chema/ and /~chema/dir/ are paths
22) Try directory listing in all the paths
23) Search for PUT, DELETE, TRACE methods in every path
24) Fingerprint software from 404 error messages
25) Fingerprint software from application error messages
26) Try common names on all domains (dictionary)
27) Try Zone Transfer on all NS
28) Search for any URL indexed by web engines related to the hostname
29) Download the file
30) Extract the metadata, hidden info and lost data
31) Sort all this information and present it nicely
32) For every new IP/URL start over again


Search All

Demo:
disa.mil

Digital Certificates

Attribute	Value
Domain - Source	
www.fcs.army.mil	Documents s
IP Addresses - Source	
143.84.29.53	Documents s
FingerPrinting - HTTP	
Version	(Unavaliable)
Version	(Unavaliable)
Version	(Unavaliable)

- usacac.army.mil_140.153.167.60.crt
- usacac.leavenworth.army.mil_140.153.167.6
- usachppm.apgea.army.mil_phc.amedd.arm
- www.49thgrp.army.mil_www.49thgrp.army
- www.alt.army.mil_www.alt.army.mil.crt
- www.apg.army.mil_www.apg.army.mil.crt
- www.arl.army.mil_ess.arl.army.mil.crt
- www.aw2.army.mil_www.aw2.army.mil.crt
- www.bands.army.mil_bands.army.mil.crt
- www.bctmod.army.mil_www.bctmod.army
- www.belvoir.army.mil_www.belvoir.army.n
- www.benning.army.mil_www.benning.arm
- www.bliss.army.mil_www.bliss.army.mil.cr
- www.carlisle.army.mil_www.carlisle.army.n
- www.crdamc.amedd.army.mil_www.crdam
- www.cs.amedd.army.mil_www.cs.amedd.a

Certificado

General | Detalles | Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Identificador de clave del tit...	09 9f 63 38 ed b5 d1 f9 3d c0 ...
Acceso a la información de ...	[1]Acceso a información de au...
Puntos de distribución CRL	[1]Punto de distribución CRL: ...
Nombre alternativo del titular	Nombre DNS=www.bctmod.ar...
Directivas del certificado	[1]Directiva de certificado:Ide...
Uso de la clave	Firma digital, Cifrado de clave ...
Algoritmo de identificación	sha1
Huella digital	41 85 b4 b1 0a e0 e5 0b 9e d9

Nombre DNS=www.bctmod.army.mil
Nombre DNS=www.fcs.army.mil

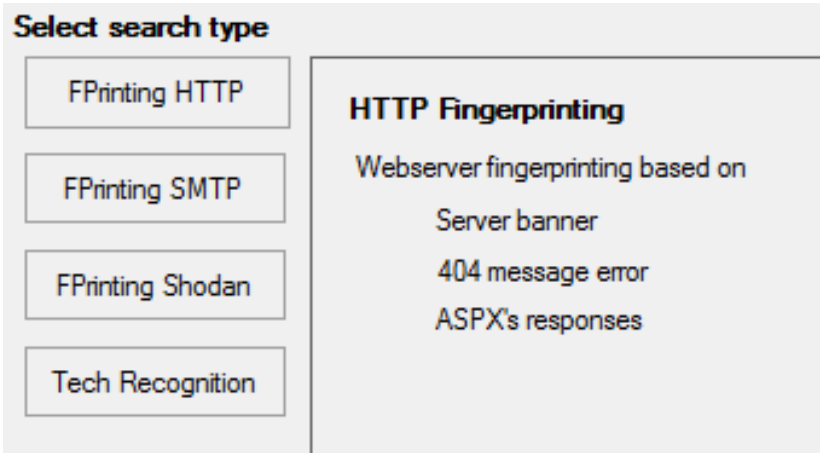
Editar propiedades... | Copiar en archivo...

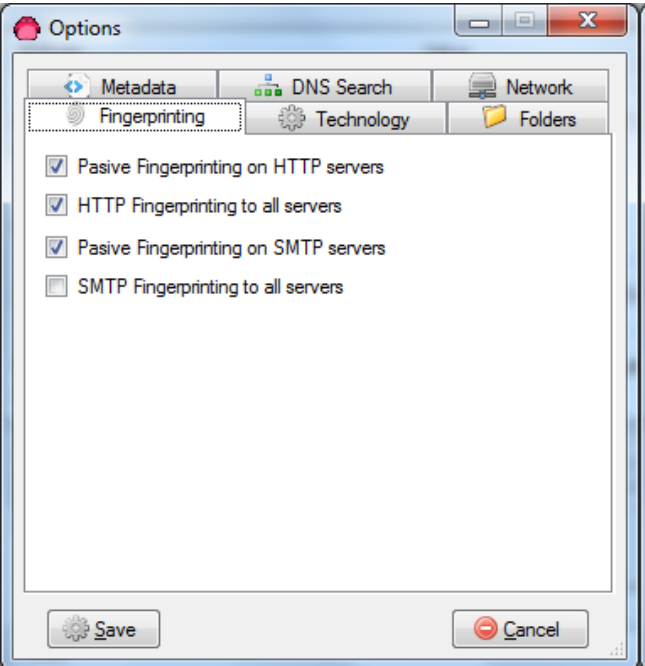
mación acerca de los detalles del certificado

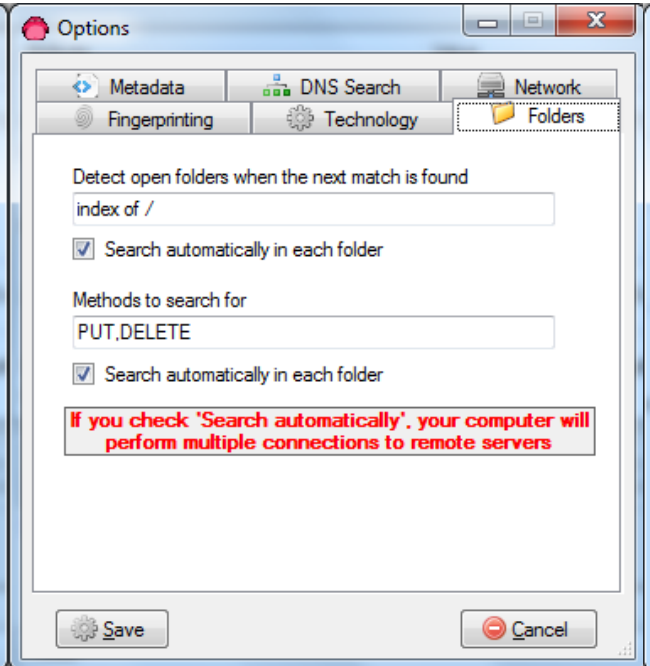
Aceptar

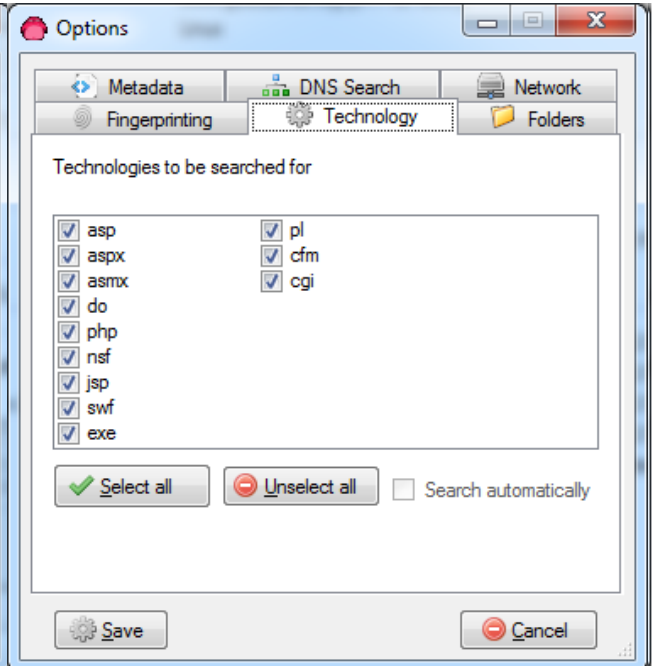
Attribute	Value
Domain - Source	
www.bctmod.army.mil	FingerPrinting
IP Addresses - Source	
143.84.29.53	Documents search > DNS resolution [143.84.29.53]
FingerPrinting - HTTP	
Version	(Unavaliable)
Version	Microsoft-IIS/6.0

FOCA 2.5 URL Analysis









Unsecure Http Methods

C:\Windows\system32\cmd.exe

```
F:\SW\netcat>nc [redacted] 80
OPTIONS /WIFI HTTP/1.x

HTTP/1.1 200 OK
Date: Wed, 23 Jun 2010 07:41:01 GMT
Server: Apache/2.0.52 (Red Hat)
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=iso-8859-1
Content-Language: es
```

Search & Upload

apple.com - FOCA Private 2.5

File | Metadata | Domain Enumeration | Software Recognition | Report | Tools | Logs | Options | About

Metadata | Network data

PCs/Servers | Domains | IPs

- pdf.euro.apple.com
- phonehome.euro.apple.com
- phonehome1.euro.apple.com
- phonehome1-bge0.euro.appl
- phonehome1-bge1.euro.appl
- phonehome2.euro.apple.com
- phonehome2-bge0.euro.appl
- phonehome2-bge1.euro.appl
- phonehome3.euro.apple.com
- phonehome3-bge0.euro.appl
- phonehome3-bge1.euro.appl
- promo1r.euro.apple.com
- promo3r.euro.apple.com
- promo4r.euro.apple.com
- registration.euro.apple.com
- sew.euro.apple.com
- streaming.euro.apple.com
- time1.euro.apple.com
- time2.euro.apple.com
- webmail.euro.apple.com
- webmail-new.euro.apple.com
- euro-red.apple.com

Attribute	Value
Domain - Source	
pdf.euro.apple.com	Reverse resolution, scaning IP range of 17.72.133.58
IP Addresses - Source	
17.72.133.33	Reverse resolution, scaning IP range of 17.72.133.58 > DNS resolution [17.72.1...
FingerPrinting - HTTP	
Version	Apache/1.3.29 (Darwin) PHP/4.3.6
Version	Apache/1.3.29 (Darwin) PHP/4.3.6

Technology Recognition | Google crawling | Search open folders | Search methods | Minimize

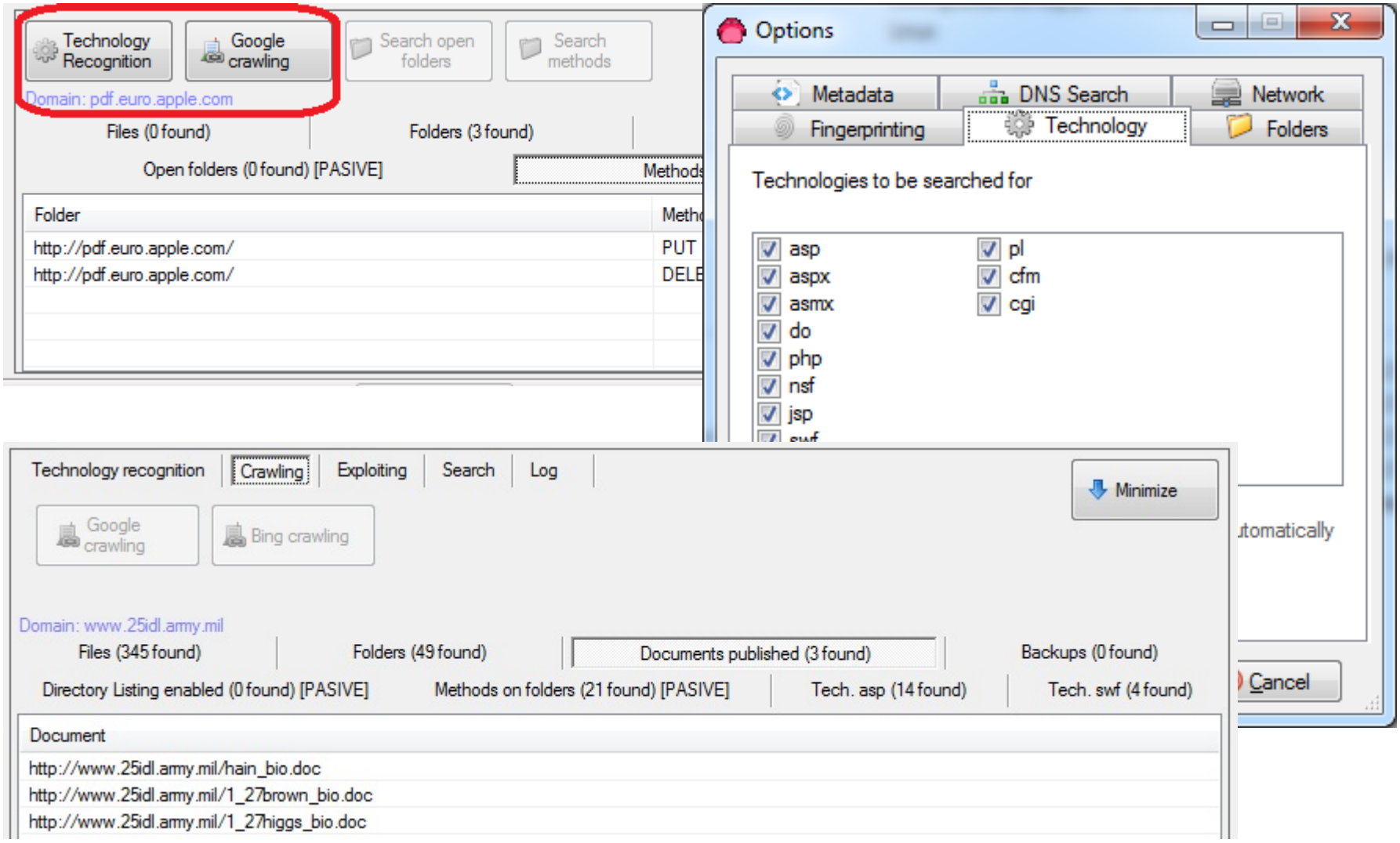
Domain: pdf.euro.apple.com

Files (0 found) | Folders (3 found) | Documents published (8 found)

Open folders (0 found) [PASIVE] | Methods on folders (2 found) [PASIVE]

Folder	Methods
http://pdf.euro.apple.com/	PUT
http://pdf.euro.apple.com/	DELETE

Searching for Server-Side Technologies



FOCA 2.5 & Shodan

SHODAN
Computer Search Engine

net:143.84.68.8 Search

Options

Save this search

Results 1 - 1 of about 1 for net:143.84.

» Top countr

143.84.68.8
NetApp Data
Added on 27.
HTTP/1.0 20
Content-len
Via: 1.1 RI
X-powered-b
X-aspnet-ve
Server: Mic
Cache-contr
Date: Fri,
Content-typ

http://shodan.surtri.com/?q=net%3A143.84.68.0/24&f=json - Windows Internet Explorer

http://shodan.surtri.com/?q=net:143.84.68.0/24&f=jso

Bing

Twitter... Blogge... http... Página Seguridad Herramientas

{"matches": [{"ip": "143.84.68.8", "updated": "27.11.2009", "hostnames": [], "data": "HTTP/1.0 200 OK\r\nContent-length: 507367\r\nVia: 1.1 RIL-CTNOSC (NetCache NetApp/6.0.2P1)\r\nX-powered-by: ASP.NET\r\nX-aspnet-version: 2.0.50727\r\nServer: Microsoft-IIS/6.0\r\nCache-control: private\r\nDate: Fri, 27 Nov 2009 06:49:36 GMT\r\nContent-type: text/html; charset=utf-8\r\n\r\n"}, {"ip": "143.84.68.5", "updated": "16.11.2009", "hostnames": [], "data": "HTTP/1.0 200 OK\r\nContent-length: 27789\r\nVia: 1.1 RIL-CTNOSC (NetCache NetApp/6.0.2P1)\r\nX-powered-by: VP1 IntraView, ASP.NET\r\nSet-cookie: ASP.NET_SessionId=fhlt0uaxmlndfwvcehq10n45; path=/\r\nX-aspnet-version: 1.1.4322\r\nServer: Microsoft-IIS/6.0\r\nCache-control: private\r\nDate: Mon, 16 Nov 2009 05:03:13 GMT\r\nContent-type: text/html; charset=utf-8\r\n\r\n"}], "total": 2, "countries": [{"count": 4, "country": "United States"}]}

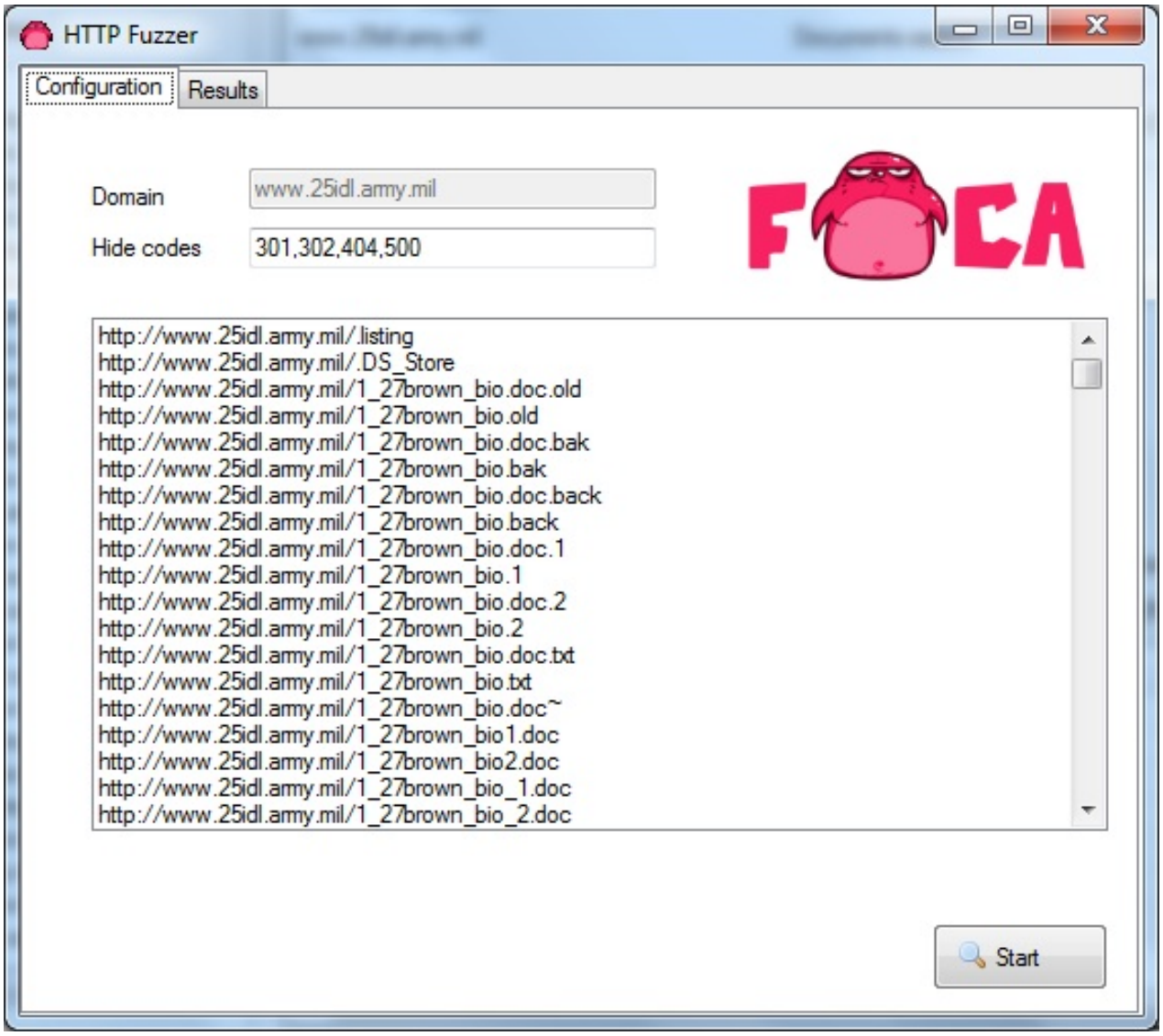
Listo

Internet | Modo protegido: activado

100%

Demo:
whitehouse.gov

Fuzzing options (PRO)



.listing

ext:listing Buscar

Aproximadamente 75.100 resultados (0,13 segundos) Búsqueda avanzada

drwxr-xr-x 3 michelo michelo 4096 Nov 7 10:31 . drwxr-x--- 23 ... - [Traducir esta página]
drwxr-xr-x 3 michelo michelo 4096 Nov 7 10:31 . drwxr-x--- 23 michelo 99 4096 Apr 20 10:22 ..
-rwxr-xr-x 1 michelo michelo 4 Apr 6 00:23 .ftpquota ...
www.index972.com/.listing - En caché

```
drwxr-xr-x   6 root     root         4096 Mar 25  2009 .
drwxr-xr-x  25 root     root         4096 May  3 17:02 ..
-rw-r--r--   1 root     root         1582 Mar 25  2009 download.mp3
drwxr-xr-x   2 root     root         4096 Mar 25  2009 getid3
drwxr-xr-x   2 root     root         4096 Mar 25  2009 images
-rw-r--r--   1 root     root        17991 Mar 25  2009 license.txt
-rw-r--r--   1 root     root          888 Mar 25  2009 mobatalk_audio_comment.php
drwxr-xr-x   4 root     root         4096 Mar 25  2009 optional_files
drwxr-xr-x   2 root     root         4096 Mar 25  2009 players
-rw-r--r--   1 root     root        22407 Mar 25  2009 podango-api.php
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 :
-rw-r--r--   1 root     root           59 Mar 25  2009 podpress_admin_tigercheck.css
-rw-r--r--   1 root     root         2123 Mar 25  2009 podpress_backend.php
-rw-r--r--   1 root     root        34228 Mar 25  2009 podpress_class.php
-rw-r--r--   1 root     root         1213 Mar 25  2009 podpress_feed.php
-rw-r--r--   1 root     root        22775 Mar 25  2009 podpress_feed_functions.php
-rw-r--r--   1 root     root        32436 Mar 25  2009 podpress_functions.php
```

ext:listing site:gov Buscar

1 resultado (0,11 segundos) Búsqueda avanzada

listing - Official NASA Fermi Website - [Traducir esta página]
drwxr-xr-x 4 4866 4915 26 Apr 03 2009 . drwxr-xr-x 5 0 0 0 Sep 23 18:45 .. drwxr-xr-x 985 4866 4915 24576 Sep 16 09:15 adp drwxr-xr-x 987 4866 4915 16384 ...
fermi.gsfc.nasa.gov/FTP/FTP/.integral_archive2/.../.listing - En caché

DNS Cache Snooping

Domain: renfe.es — Obtain DNS servers

File: C:\Users\i64\AppData\Local\Apps\2.0\LGA16CMW.3TW\LBE5TQYE.Z0M\foca..tion_e — Load file

Dns: Snoop DNS

- ns1.renfe.es
- dns1.renfe.es
- dns2.renfe.es
- ns2.renfe.es

Cache

Host
Default
www.facebook.com
facebook.com
twitter.com
update.microsoft.com
www.periodistadigital.com
elladodelmal.blogspot.com
www.informatica64.com
megaupload.com

Monitor

Host	First	Last
Default		
www.facebook.com	15:55	15:55
facebook.com	15:55	15:55
twitter.com	15:55	15:55
update.microsoft.com	15:55	15:55
www.periodistadigital.com	15:55	15:55
elladodelmal.blogspot.com	15:55	15:55
www.informatica64.com	15:55	15:55
megaupload.com	15:55	15:55

☐ Monitorice each 60 seconds

DNS Cache Snooping

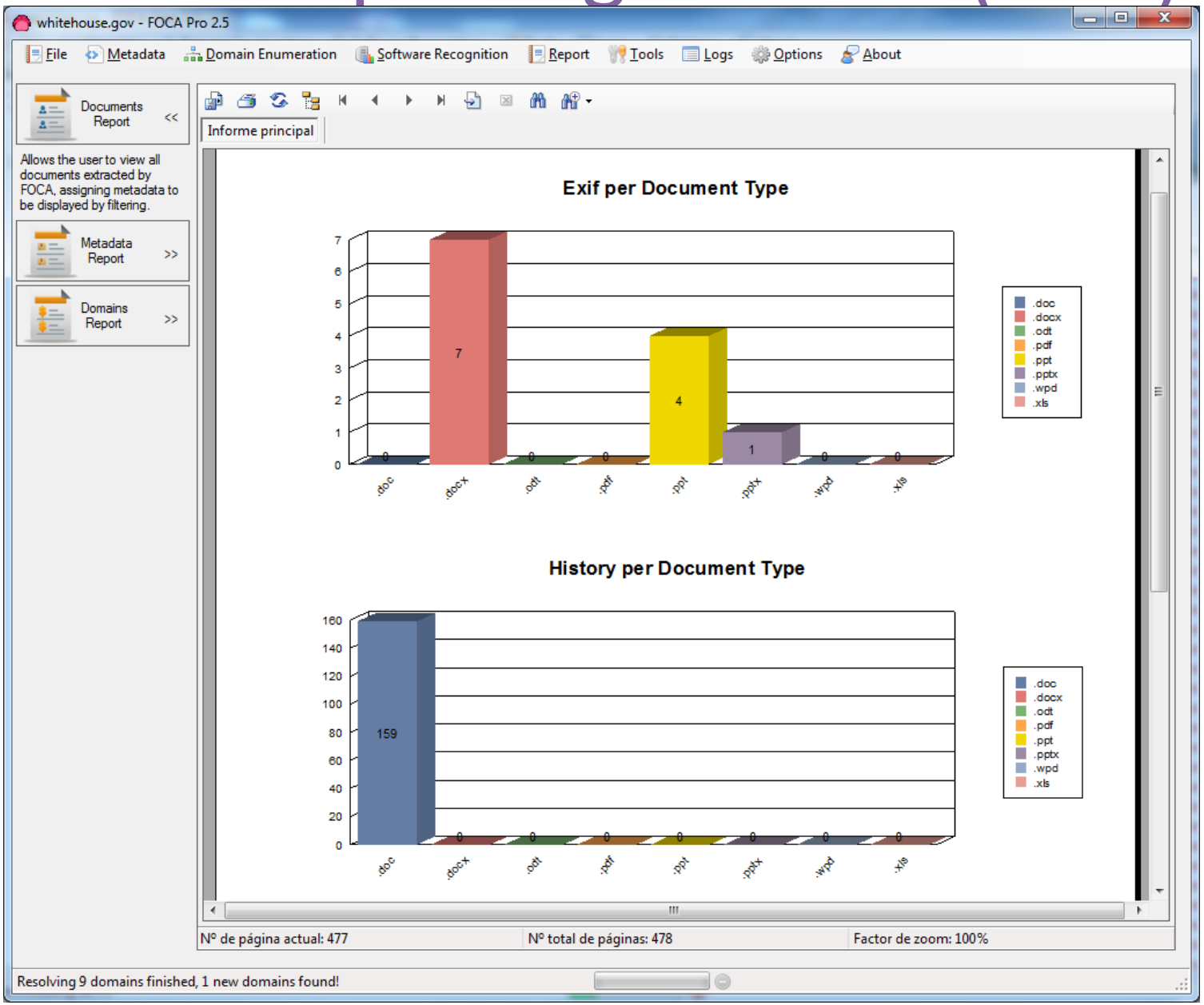
```
C:\>nslookup
Servidor predeterminado:  UnKnown
Address:  192.168.1.1

> set type=ns
> renfe.es
Servidor:  UnKnown
Address:  192.168.1.1

Respuesta no autoritativa:
renfe.es        nameserver = dns1.renfe.es
renfe.es        nameserver = dns2.renfe.es
renfe.es        nameserver = ns1.renfe.es
renfe.es        nameserver = ns2.renfe.es

dns1.renfe.es   internet address = 213.144.49.35
dns2.renfe.es   internet address = 213.144.49.43
ns1.renfe.es    internet address = 213.144.33.254
> server ns1.renfe.es
Servidor predeterminado:  ns1.renfe.es
Address:  213.144.33.254
```

```
> set type=a
> set norecurse
> www.facebook.com
Servidor:  ns1.renfe.es
Address:  213.144.33.254

Respuesta no autoritativa:
Nombre:  www.facebook.com
Address:  69.63.190.18

> elladodelmal.blogspot.com
Servidor:  ns1.renfe.es
Address:  213.144.33.254

Nombre:  elladodelmal.blogspot.com
Served by:
- ns3.google.com
            216.239.36.10
            blogspot.com
- ns4.google.com
```

DNS Cache Snooping

- Internal Software
  - Windows Update
  - Gtalk
- Evilgrade
  - Detecting vulnerable software to Evilgrade attacks
- AV evassion
  - Detecting internal AV systems
- Malware driven by URL
  - Hacking a web site ussually visited by internal users

FOCA Reporting Module (PRO)



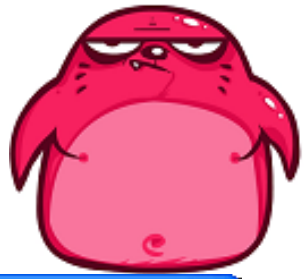
Demo: DNS
Cache Snooping

Fear The FOCA

FOCA on Linux?

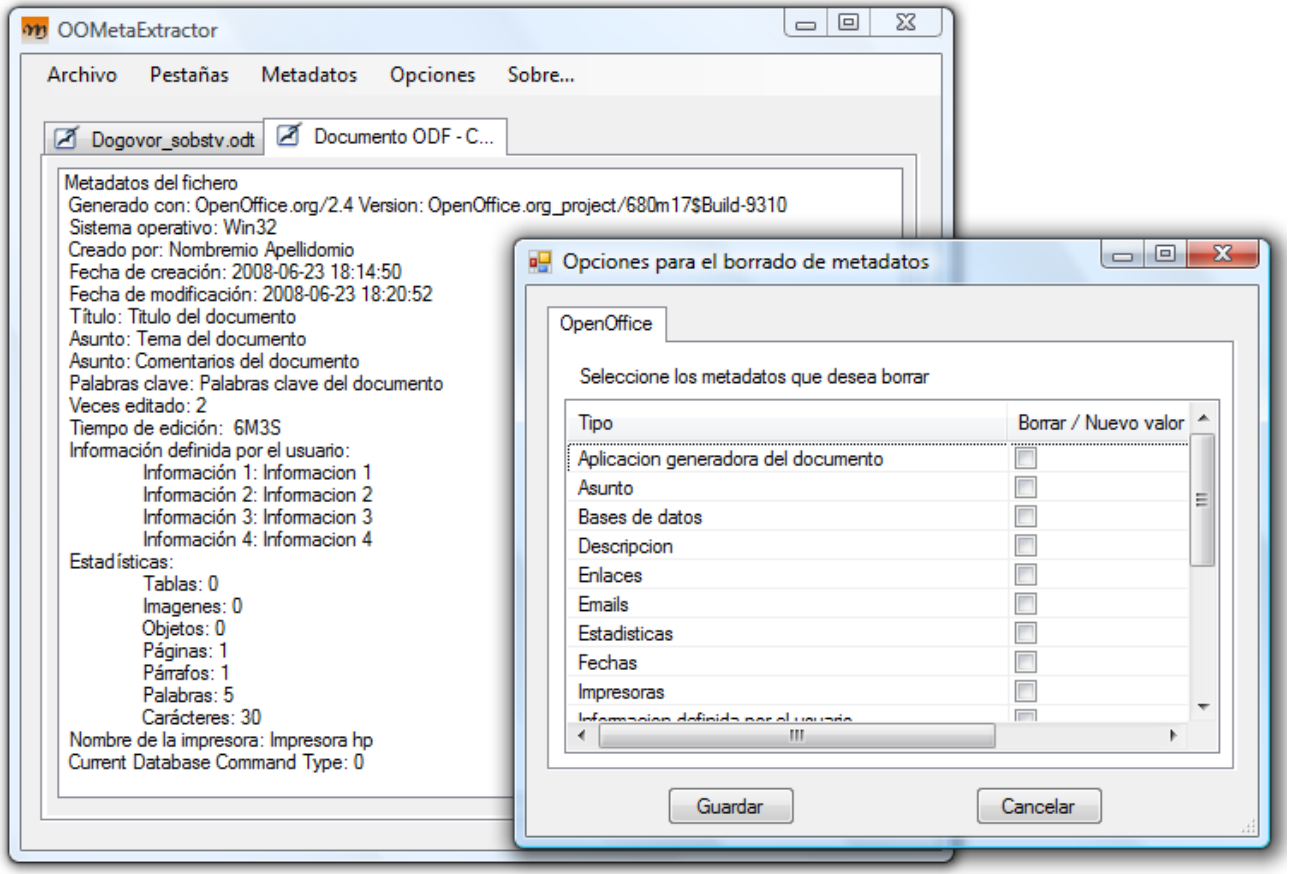
FOCA Online

http://www.informatica64.com/FOCA



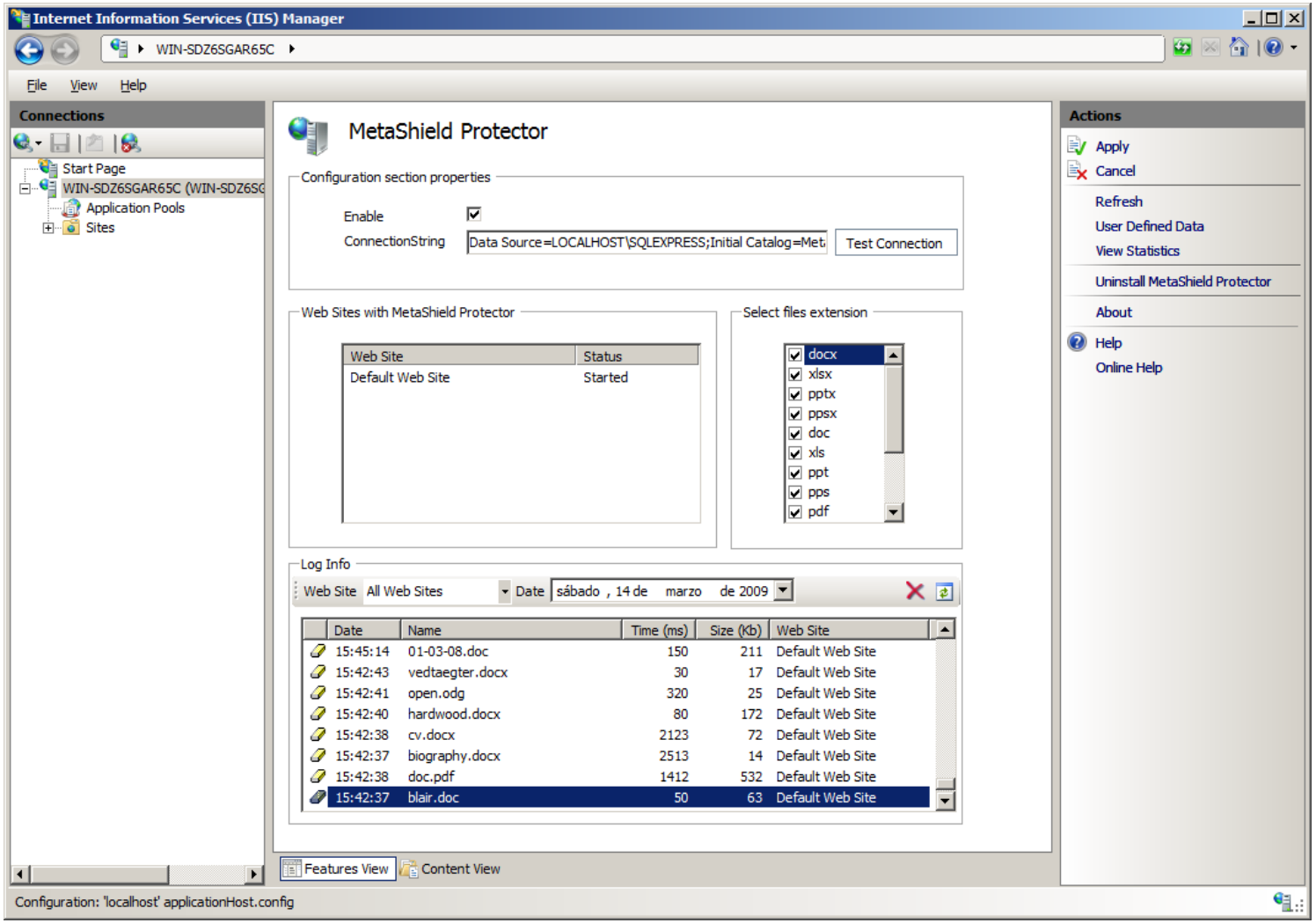
Cleaning documents

- OOMetaExtractor



http://www.codeplex.org/oometaextractor

IIS MetaShield Protector



http://www.metashieldprotector.com

Get FOCA!

- FOCA Free 2.6.1
  - http://www.informatica64.com/FOCA
- Love FOCA and want the Pro Version?
  - Book for an online training! (28th April)
  - http://www.informatica64.com/DownloadFOCA/Trainings.aspx
- Have the Pro version but not the last version?
  - Help FOCA
    - Spread the word!
    - Buy a FOCA T-Shirt
    - Buy me something to drink

Buy a FOCA T-Shirt

And be «Sexy» }:))

Questions?

- Chema Alonso
  - chema@informatica64.com
  - http://www.informatica64.com
  - http://www.elladodelmal.com
  - http://twitter.com/chemaalonso
  - http://www.forefront-es.com
  - http://www.seguridadapple.com
  - http://www.windowstecnico.com
  - http://www.puntocompartido.com
- Working on FOCA:
  - Chema Alonso
  - Alejandro Martín
  - Francisco Oca
  - Manuel Fernández «The Sur»
  - Daniel Romero
  - Enrique Rando
  - Pedro Laguna
  - Special Thanks to: John Matherly [Shodan]