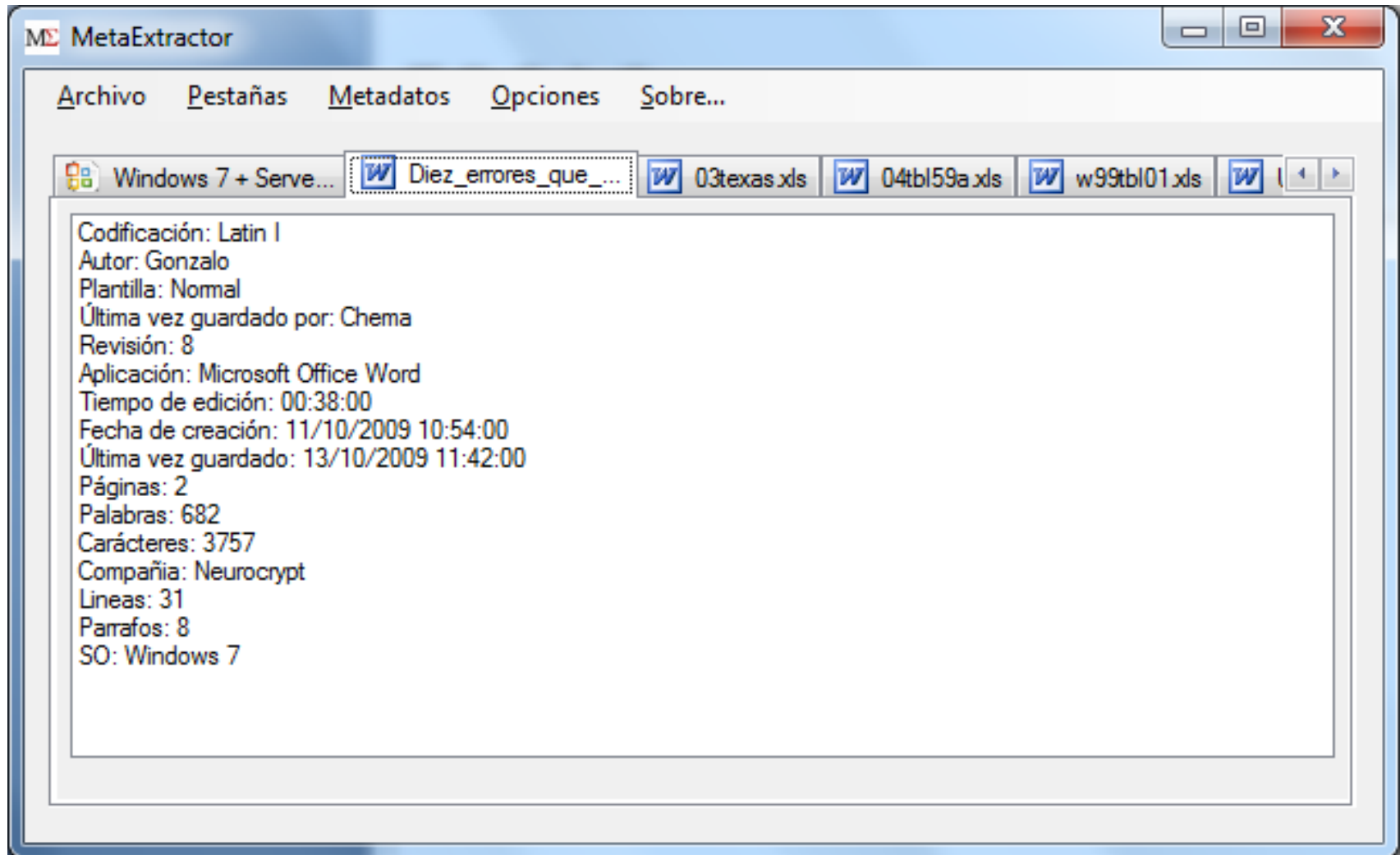


# La Gorda FOCA

Chema Alonso



# FOCA 0.x



# Foca 1 : Análisis de Metadatos

- Busca documentos en Google y Bing
- Descarga los documentos
- Extrae los metadatos
- Clusteriza los documentos
- Genera un mapa de red

## FOCA 1: Metadatos

- Usuarios:
  - Creadores.
  - Modificadores .
  - Usuarios en paths.
    - C:\Documents and settings\jfoo\myfile
    - /home/johnnyf
- Sistemas Operativos
- Impresoras
  - Locales y remotas.
- Paths.
  - Locales y remotos.
- Información de red.
  - Shared Printers.
  - Shared Folders.
  - ACLS.
- Internal Servers.
  - NetBIOS Name.
  - Domain Name.
  - IP Address.
- Estructuras de BBDD.
  - Table names.
  - Colum names.
- Devices info.
  - Mobiles.
  - Photo cameras.
- Private Info.
  - Personal data.
- Historial de uso.
- Versiones de software.

# **ALGUNOS EJEMPLOS**

# FOCA 1: Post-Post-Análisis

- Google Set
- Alternative Domains
- Robtex
- Rango IP
- DNS Prediction

# Google Sets

/Rooted<sup>®</sup>  
2010



Predicted Items	
<a href="#">poland</a>	<a href="#">spain</a>
<a href="#">germany</a>	<a href="#">slovakia</a>
<a href="#">hungary</a>	<a href="#">belgium</a>
<a href="#">france</a>	<a href="#">sweden</a>
<a href="#">italy</a>	<a href="#">denmark</a>
<a href="#">austria</a>	<a href="#">switzerland</a>
<a href="#">russia</a>	<a href="#">finland</a>
<a href="#">spain</a>	<a href="#">netherlands</a>
<a href="#">slovakia</a>	<a href="#">portugal</a>
<a href="#">belgium</a>	<a href="#">greece</a>
<a href="#">sweden</a>	<a href="#">romania</a>
<a href="#">denmark</a>	<a href="#">norway</a>
<a href="#">switzerland</a>	<a href="#">slovenia</a>
	<a href="#">ireland</a>



## DNS Scanning

novell.com - FOCA 0.9.1.0

File Search files Analyze Metadata Options About

Project Network data

novell.com

- PC\_Binoy Thomas
- Users
- Folders
- blr-nm-r14g.blr.novell.com [164.99.164.7]
- blr-nm-r14a.blr.novell.com [164.99.164.1]
- blr-nm-r14b.blr.novell.com [164.99.164.2]
- blr-nm-r14c.blr.novell.com [164.99.164.3]
- blr-nm-r14d.blr.novell.com [164.99.164.4]
- blr-nm-r14e.blr.novell.com [164.99.164.5]
- blr-nm-r14f.blr.novell.com [164.99.164.6]
- blr-nm-r14h.blr.novell.com [164.99.164.8]
- blr-nm-r15a.blr.novell.com [164.99.164.9]
- blr-nm-r15b.blr.novell.com [164.99.164.10]
- blr-nm-r15c.blr.novell.com [164.99.164.11]
- blr-nm-r15d.blr.novell.com [164.99.164.12]
- blr-nm-r15e.blr.novell.com [164.99.164.13]
- blr-nm-r15f.blr.novell.com [164.99.164.14]
- blr-nm-r15g.blr.novell.com [164.99.164.15]
- blr-nm-r15h.blr.novell.com [164.99.164.16]
- blr-nm-r16a.blr.novell.com [164.99.164.17]
- blr-nm-r16b.blr.novell.com [164.99.164.18]
- blr-nm-r16c.blr.novell.com [164.99.164.19]
- blr-nm-r16d.blr.novell.com [164.99.164.20]

Attribute	Value
<b>Information</b>	
Name	blr-nm-r14g.blr.novell.com
IP	164.99.164.7
<b>Remote Users</b>	
Username	Binoy Thomas
<b>Documents used to infer this computer</b>	
Document	zlmagent_autoyst_inst.odt

Metadata analyzed !

## Alternate Domains

novell.com - FOCA 0.9.1.0

File Search files Analyze Metadata Options About

Project Network data

novell.com

- PC\_Binoy Thomas
  - Users
  - Folders
  - blr-nm-r14g.blr.novell.com [164.99.164.7]
  - blr-nm-r14a.blr.novell.com [164.99.164.1]
  - blr-nm-r14b.blr.novell.com [164.99.164.2]
  - blr-nm-r14c.blr.novell.com [164.99.164.3]
  - blr-nm-r14d.blr.novell.com [164.99.164.4]
  - blr-nm-r14e.blr.novell.com [164.99.164.5]
  - blr-nm-r14f.blr.novell.com [164.99.164.6]
  - blr-nm-r14h.blr.novell.com [164.99.164.8]
  - blr-nm-r15a.blr.novell.com [164.99.164.9]
  - blr-nm-r15b.blr.novell.com [164.99.164.10]
  - blr-nm-r15c.blr.novell.com [164.99.164.11]
  - blr-nm-r15d.blr.novell.com [164.99.164.12]
  - blr-nm-r15e.blr.novell.com [164.99.164.13]
  - blr-nm-r15f.blr.novell.com [164.99.164.14]
  - blr-nm-r15g.blr.novell.com [164.99.164.15]
  - blr-nm-r15h.blr.novell.com [164.99.164.16]
  - blr-nm-r16a.blr.novell.com [164.99.164.17]
  - blr-nm-r16b.blr.novell.com [164.99.164.18]
  - blr-nm-r16c.blr.novell.com [164.99.164.19]
  - blr-nm-r16d.blr.novell.com [164.99.164.20]

Attribute	Value
<b>Information</b>	
Name	blr-nm-r14g.blr.novell.com
IP	164.99.164.7
<b>Remote Users</b>	
Username	Binoy Thomas
<b>Documents used to infer this computer</b>	
Document	zlmagent_autoyst_inst.odt

## DNS Prediction

**Add variable**

Position  
www{0}.usal.es

Start value 0 End value 9

Add

**DNS Prediction**

Pattern  
www{0}.usal.es

Variables

Variable	Values
{0}	0 - 9

Nº Variants: 10

Scan

**FOCA RC1**

File Search files Analyze Metadata Options About

Project Network data

- Clients
  - PC\_jisbister
- Servers
  - ecf.mdd.uscourts.gov [207.41.16.93]
  - www1.usal.es [212.128.129.17]
  - www2.usal.es [212.128.129.43]
  - www3.usal.es [212.128.129.120]
  - ftp1.usal.es [212.128.130.49]

Attribute

**Information**

Name

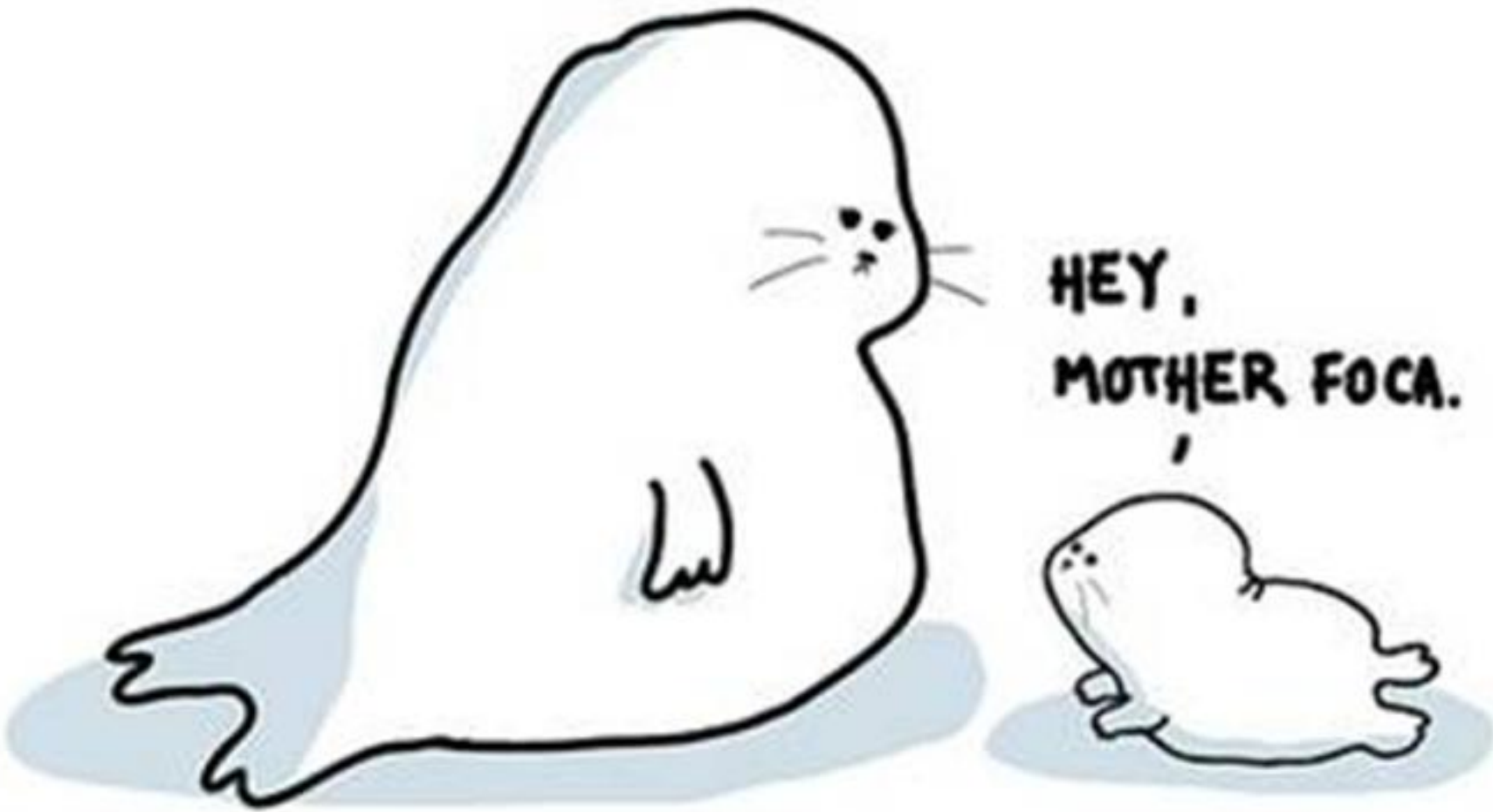
IP

## Problemas para pintar la red

- Alternative domains:
  - O los sabías o aparecían o el servidor queda sin dominio.
- DNS Scanning:
  - Si el equipo no tiene dominio -> no tienes IP no puedes aplicar DNS scanning
- Google Sets
  - Si no hay dominio, aunque encuentres nombres similares no sabes contra que dns probarlo.

# FOCA 2.0 aún en alpha

/Rooted<sup>®</sup>  
2010



adrs

## Necesitamos dominios

### [Partido Socialista Obrero Español - PSOE](#)

Partido Socialista. Presentación Secretario General · Nuestras Ideas y Valores · Historia · Estructura · Instituciones · Resultados electorales ...

<https://www.psoe.es/> - [En caché](#) - [Similares](#)

### [El Gobierno se comprometió a licitar y financiar el emisario - PSOE](#)

PSOE, El Gobierno se comprometió a licitar y financiar el emisario, El intendente Katz firmó ayer un convenio marco con Obras de la Nación.

<mardelplata.psoe.es/> - [En caché](#) - [Similares](#)

### [Agrupación Socialista de Oviedo, Agrupación Socialista de Oviedo ...](#)

Información de la agrupación y grupo municipal, con documentación y noticias.

<oviedo.psoe.es/> - [En caché](#) - [Similares](#)

### [Agrupación Socialista de Alcalá de Henares, Agrupación Socialista ...](#)

PSOE, Agrupación Socialista de Alcalá de Henares, Agrupación Socialista de Alcalá de Henares Madrid - Noticias,

<alcaladehenares.psoe.es/> - [En caché](#) - [Similares](#)

### [Laicidad, libertad de conciencia y religiosa, Laicidad, libertad ...](#)

PSOE, Laicidad, libertad de conciencia y religiosa, Laicidad, libertad de conciencia y religiosa - Noticias,

<laicidad.psoe.es/> - [En caché](#) - [Similares](#)

### [Agrupación Socialista de Chamberí, Agrupación Socialista de ...](#)

PSOE, Agrupación Socialista de Chamberí, Agrupación Socialista de Chamberí - Noticias,

<www.chamberi.psoe.es/> - [En caché](#) - [Similares](#)

### [Málaga Puerto de la Torre - Teatinos, Málaga Puerto de la Torre ...](#)

PSOE, Málaga Puerto de la Torre - Teatinos, Málaga Puerto de la Torre- Teatinos - Noticias,

<puertotorre.psoe.es/> - [En caché](#)

# Cómo buscar dominios

- Metadatos [SetA]
    - Aparece el nombre dominio
    - Aparece la dirección IP -> Resolución DNS
  - Google & Bing Search [SetB]
    - Uso de site y –inurl para maximizar resultados
- Se obtienen Domain names [SetA+SetB]

## Direcciones IPs

- Metadatos [IP\_A]
    - Direcciones IP directamente
    - Nombres completos -> Resolución DNS contra DNS principal del dominio.
  - Nombres Dominio Google & BING [IP\_B]
    - Resolución DNS
- Se obtienen direcciones IP [IP\_A+IP\_B]



# Más dominios: Bing Search IP

- Con [IP\_A+IP\_B]
  - Bing Search con parámetro IP
  - > Nuevos dominios
    - Internos
    - Relacionados

## Mas dominios: PTR Scanning

- Con todas las direcciones IP
  - Conexión al NS principal [Opcional a todos los NS]

```
C:\Windows\system32\cmd.exe - nslookup

> set type=ns
> urjc.es

Respuesta no autoritativa:
urjc.es nameserver = orion.urjc.es
urjc.es nameserver = sun.rediris.es
urjc.es nameserver = deimos.urjc.es
urjc.es nameserver = neptuno.urjc.es
urjc.es nameserver = chico.rediris.es
urjc.es nameserver = cibeles.urjc.es
urjc.es nameserver = saturno.urjc.es
urjc.es nameserver = titan.urjc.es

sun.rediris.es internet address = 130.206.1.2
neptuno.urjc.es internet address = 193.147.184.2
chico.rediris.es internet address = 130.206.1.3
saturno.urjc.es internet address = 193.147.184.11
> server neptuno.urjc.es
Servidor predeterminado: neptuno.urjc.es
Address: 193.147.184.2

> set type=ptr
>
```

## Mas dominios: PTR Scanning

```
> 192.168.46.21
Servidor: titan.urjc.es
Address: 193.147.69.2
21.46.168.192.in-addr.arpa      name = morgana.urjc.es
46.168.192.in-addr.arpa nameserver = neptuno.urjc.es
46.168.192.in-addr.arpa nameserver = saturno.urjc.es
46.168.192.in-addr.arpa nameserver = orion.urjc.es
46.168.192.in-addr.arpa nameserver = titan.urjc.es
46.168.192.in-addr.arpa nameserver = deimos.urjc.es
46.168.192.in-addr.arpa nameserver = cibeles.urjc.es
orion.urjc.es      internet address = 212.128.2.50
titan.urjc.es      internet address = 193.147.69.2
deimos.urjc.es     internet address = 193.147.184.69
cibeles.urjc.es    internet address = 193.147.64.106
neptuno.urjc.es    internet address = 193.147.184.2
saturno.urjc.es    internet address = 193.147.184.11
> 192.168.46.22
Servidor: titan.urjc.es
Address: 193.147.69.2
22.46.168.192.in-addr.arpa      name = ares.urjc.es
46.168.192.in-addr.arpa nameserver = cibeles.urjc.es
46.168.192.in-addr.arpa nameserver = neptuno.urjc.es
46.168.192.in-addr.arpa nameserver = saturno.urjc.es
46.168.192.in-addr.arpa nameserver = orion.urjc.es
46.168.192.in-addr.arpa nameserver = titan.urjc.es
46.168.192.in-addr.arpa nameserver = deimos.urjc.es
orion.urjc.es      internet address = 212.128.2.50
titan.urjc.es      internet address = 193.147.69.2
deimos.urjc.es     internet address = 193.147.184.69
cibeles.urjc.es    internet address = 193.147.64.106
neptuno.urjc.es    internet address = 193.147.184.2
saturno.urjc.es    internet address = 193.147.184.11
```

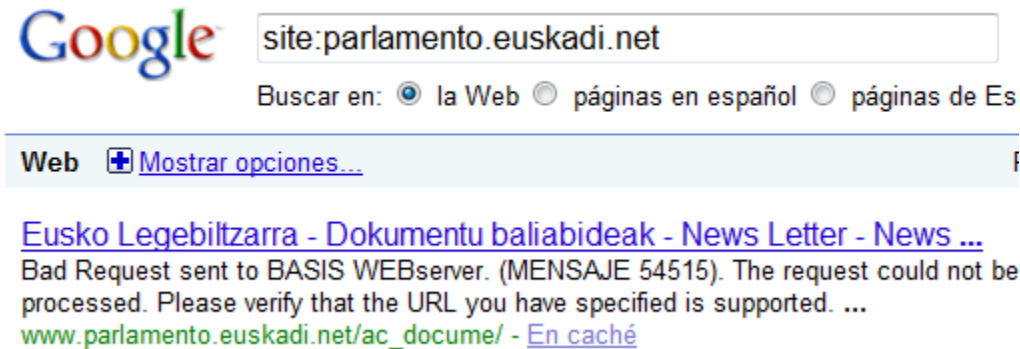
## Más dominios: Rango IP

- Todas las direcciones IP asociadas a un dominio objetivo:
  - Resolución y Búsqueda del rango con el DNS interno.
  - Opcionalmente con todos los NS

## Más dominios + Más IPs

- Common names
  - ftp, dns, dns01, pc01...
- Uso del “ls” en el DNS

## Algoritmo recursivo



```
C:\>ping www.parlamento.euskadi.net  
Haciendo ping a www.parlamento.euskadi.net [195.55.245.122]  
5:
```

```
C:\>ping -a 195.55.245.112  
Haciendo ping a parla001.parlam.euskadi.net [195.55.245.112]  
5:
```

## Algoritmo recursivo:

Aplica “algoritmo voraz”

Sigue todos los caminos

Profundidad del algoritmo es configurable

Detecta casi todas las referencias accesibles

```
C:\>ping parla011.parlam.euskadi.net  
Haciendo ping a parla011.parlam.euskadi.net [195.55.245.122]  
os:  
Control-C  
^C  
C:\>ping -a 212.55.31.242  
Haciendo ping a parla011.parlam.euskadi.net [212.55.31.242]  
s:  
t:
```

# FOCA & SHODAN

/Rooted<sup>®</sup>  
2010

The image shows the SHODAN Computer Search Engine interface. The search bar contains the query "net:143.84.68.8" and a "Search" button. Below the search bar is an "Options" button. A "Save this search" button is also visible. The results section shows "Results 1 - 1 of about 1 for net:143.84.68.8".

A Windows Internet Explorer window is overlaid on the SHODAN interface, displaying the search results in JSON format. The address bar shows the URL "http://shodan.surtri.com/?q=net%3A143.84.68.0/24&f=json". The search results are as follows:

```
{
  "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"
    }
  ]
}
```

The status bar at the bottom of the Internet Explorer window shows "Internet | Modo protegido: activado" and a zoom level of "100%".



# **ALGUNA DEMO CON FOCA 2**

FOCA sólo corre en Windows

/Rooted<sup>®</sup>  
2010



# Evolución: SW recognition

- Metadatos
  - Rutas de instalación [mejorado]
  - OLE Streams
  - EXIF
- SHODAN
  - Banners [No intrusivo]
- Banners
  - Connect
- URLs
  - Google Hacking
- NameServers
  - Prediction

Más de 20.000 FOCA's

**/Rooted<sup>®</sup>**  
**2010**



Chema Alonso

[chema@informatica64.com](mailto:chema@informatica64.com)

<http://elladodelmal.blogspot.com>

<http://twitter.com/chemaalonso>

<http://www.informatica64.com>

Autores

Chema Alonso

Francisco Oca

Alejandro Martín Bailón

Enrique Rando

Pedro Laguna

John Matherly