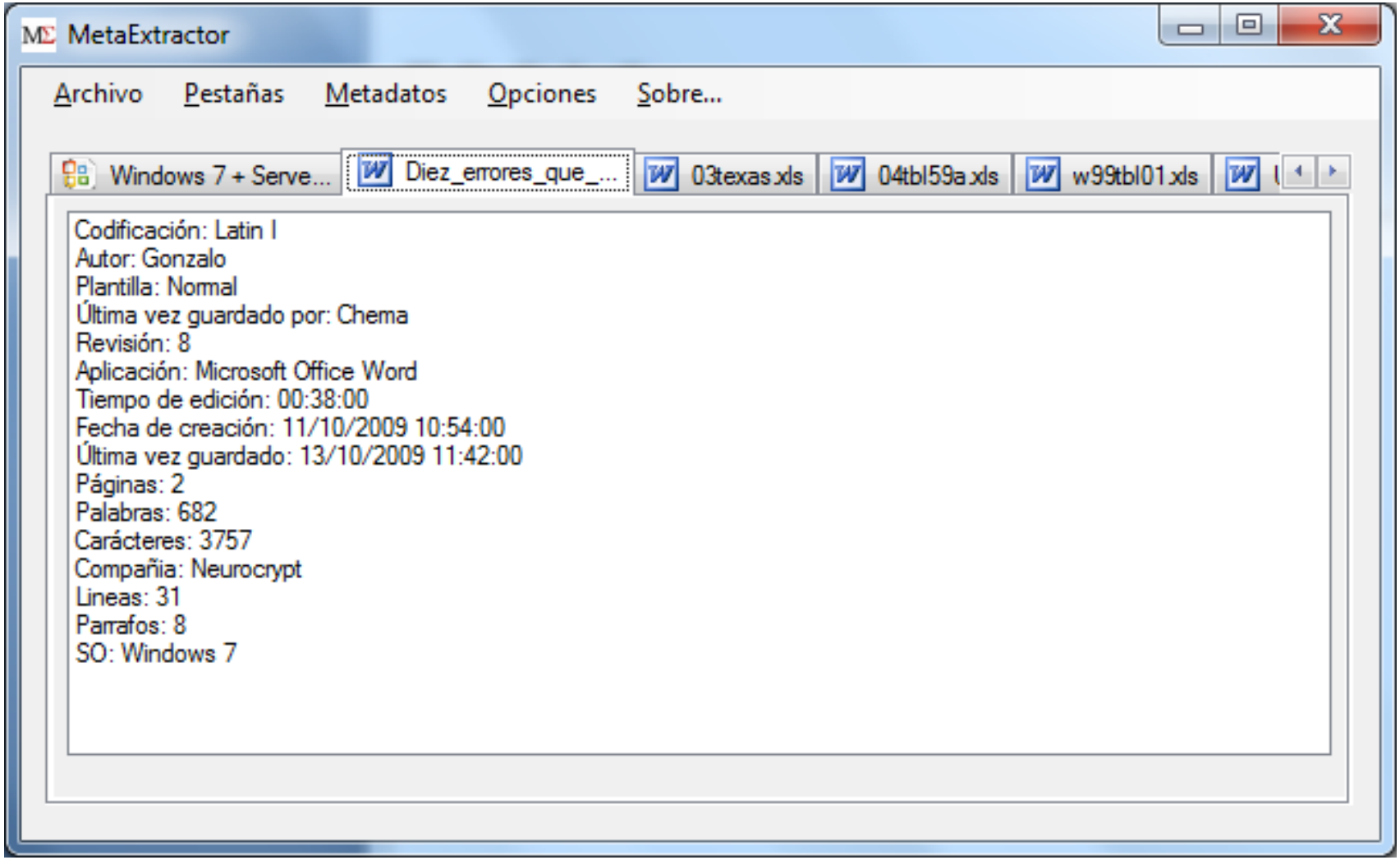
/Rooted 2010

La Gorda FOCA

Chema Alonso

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

Foca 1 : Análisis de Metadatos

/Rooted 2010

- 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

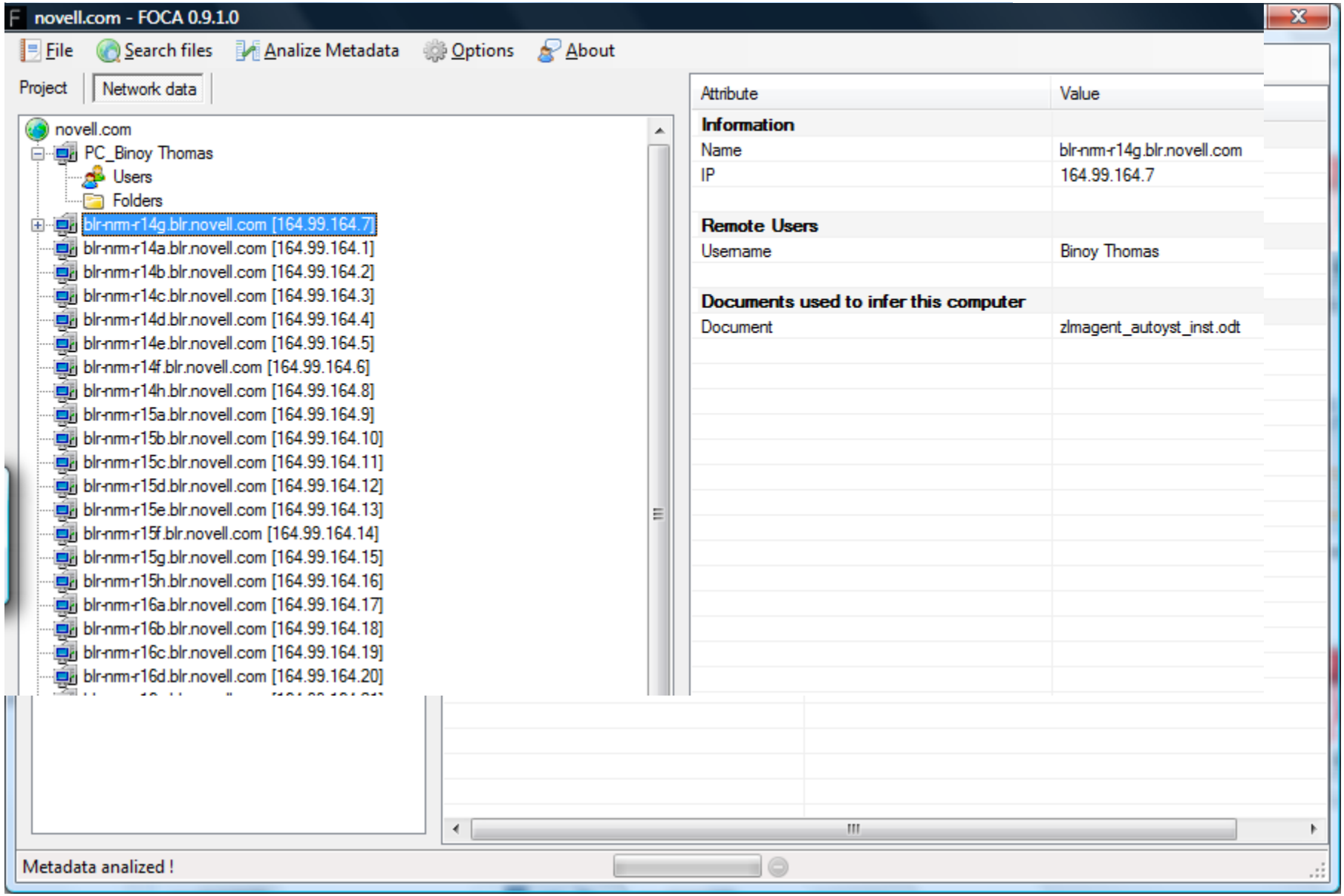
- Google Set
- Alternative Domains
- Robtex
- Rango IP
- DNS Prediction

Google Sets

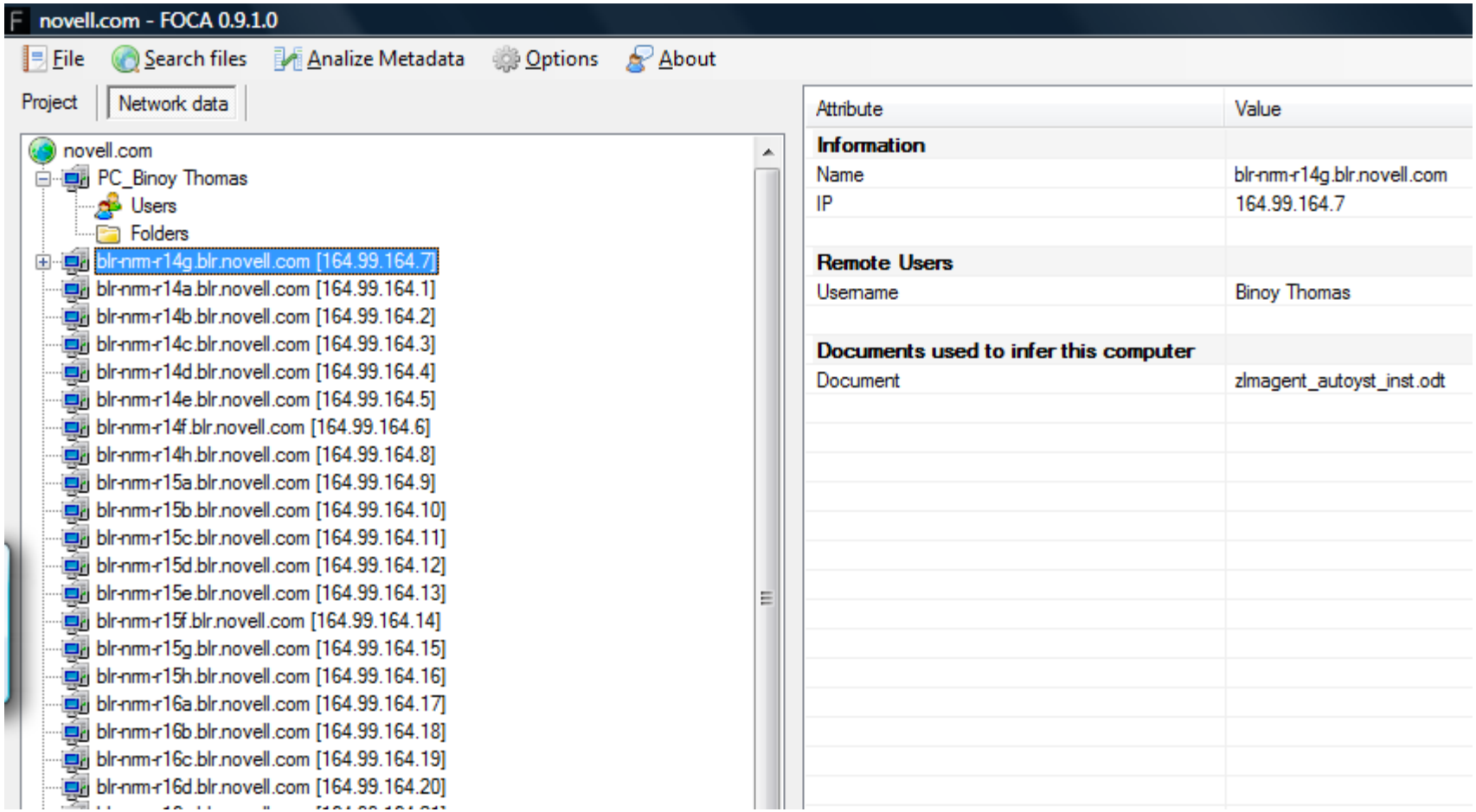
Predicted Items
poland
germany
hungary
france
italy
austria
russia
spain
slovakia
belgium
sweden
denmark
switzerland

spain
slovakia
belgium
sweden
denmark
switzerland
finland
netherlands
portugal
greece
romania
norway
slovenia
ireland

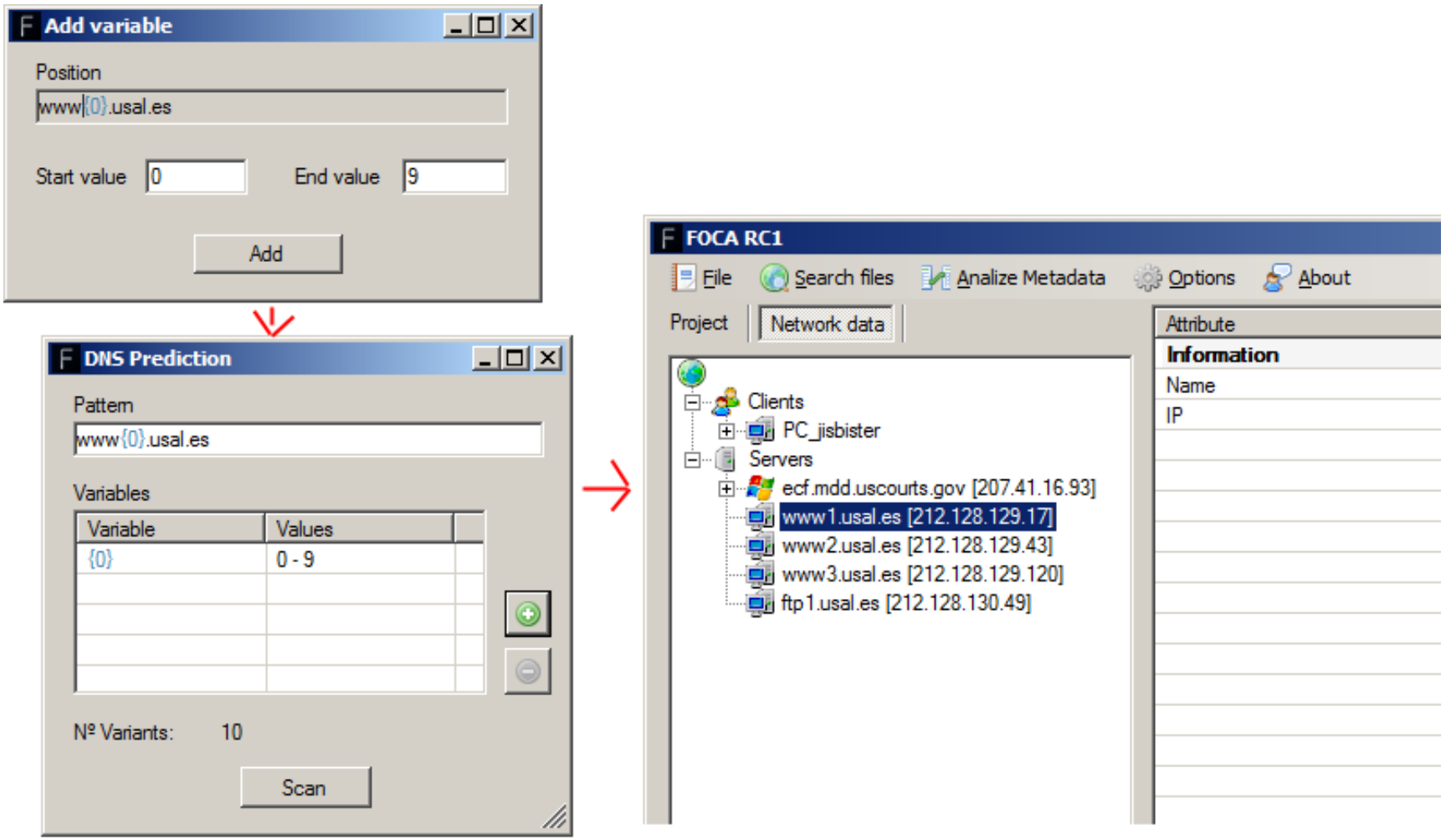
DNS Scanning



Alternate Domains



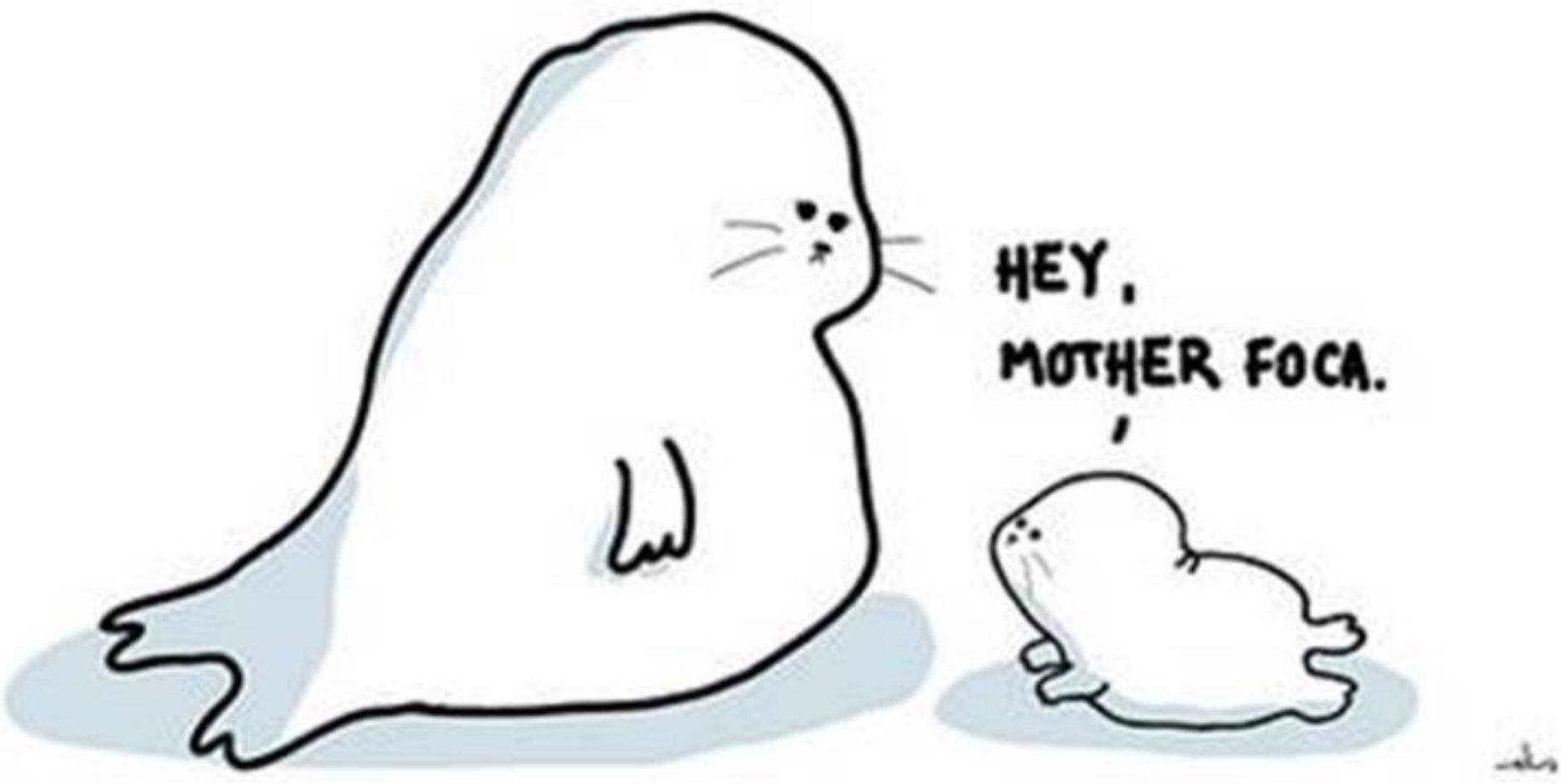
DNS Prediction



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



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

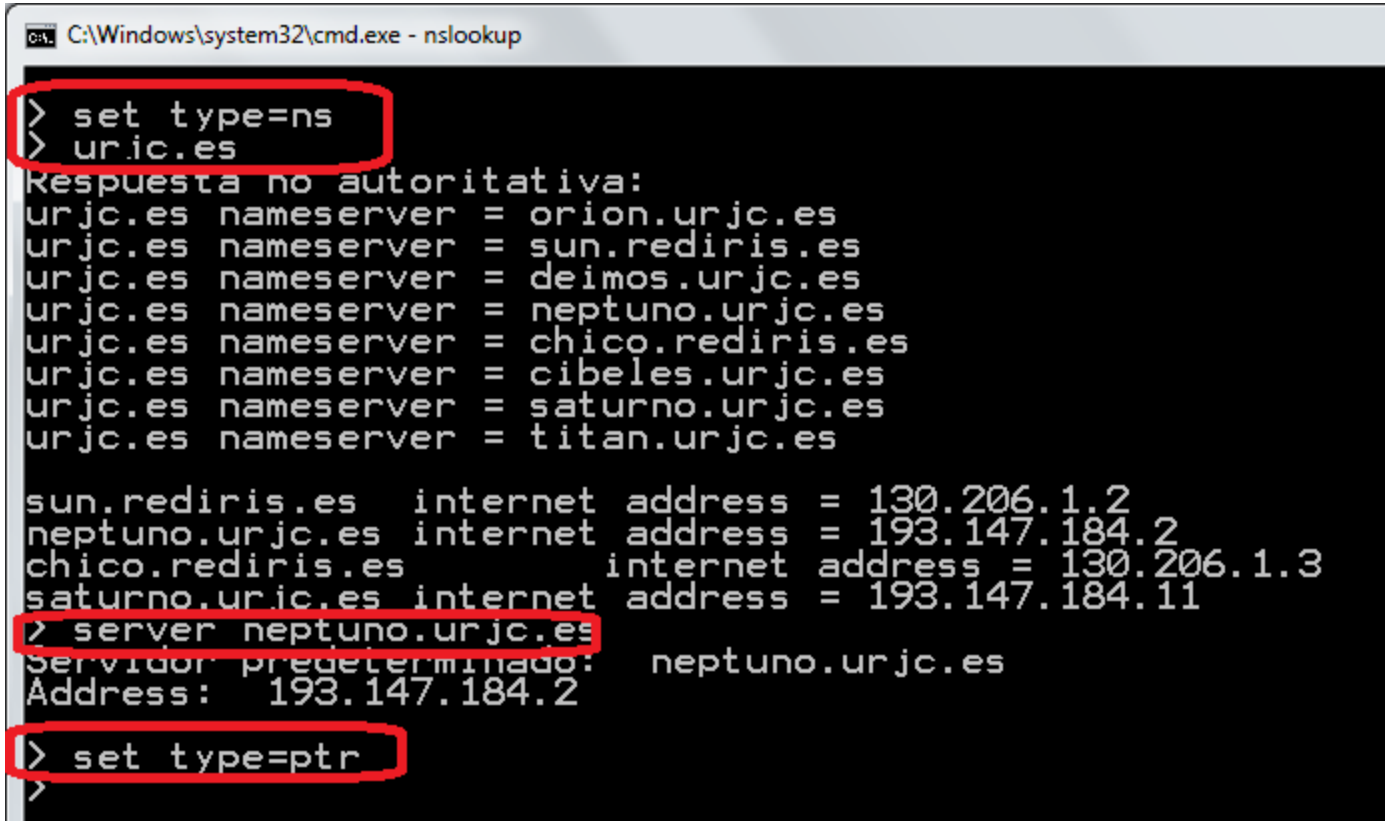
→ Se obtienen direcciones IP [IP_A+IP_B]

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]



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 = 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 = 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
```

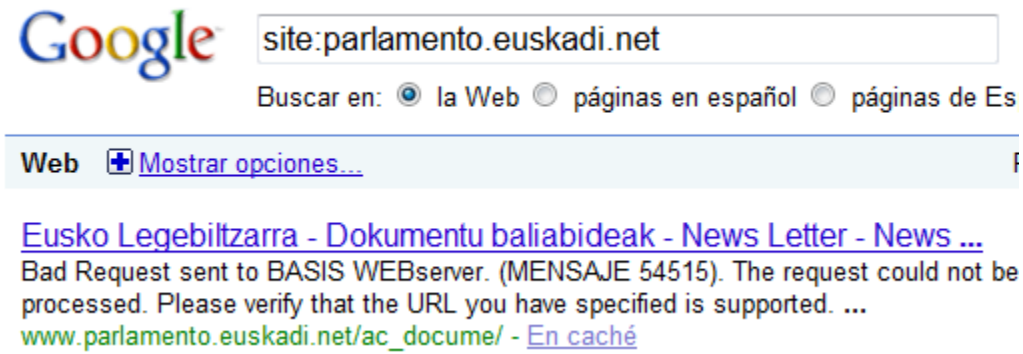
Más dominios: Rango IP

- 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]
s:
```

```
C:\>ping -a 195.55.245.112

Haciendo ping a parla001.parlam.euskadi.net [195.55.245.112]
```

Algoritmo recursivo:

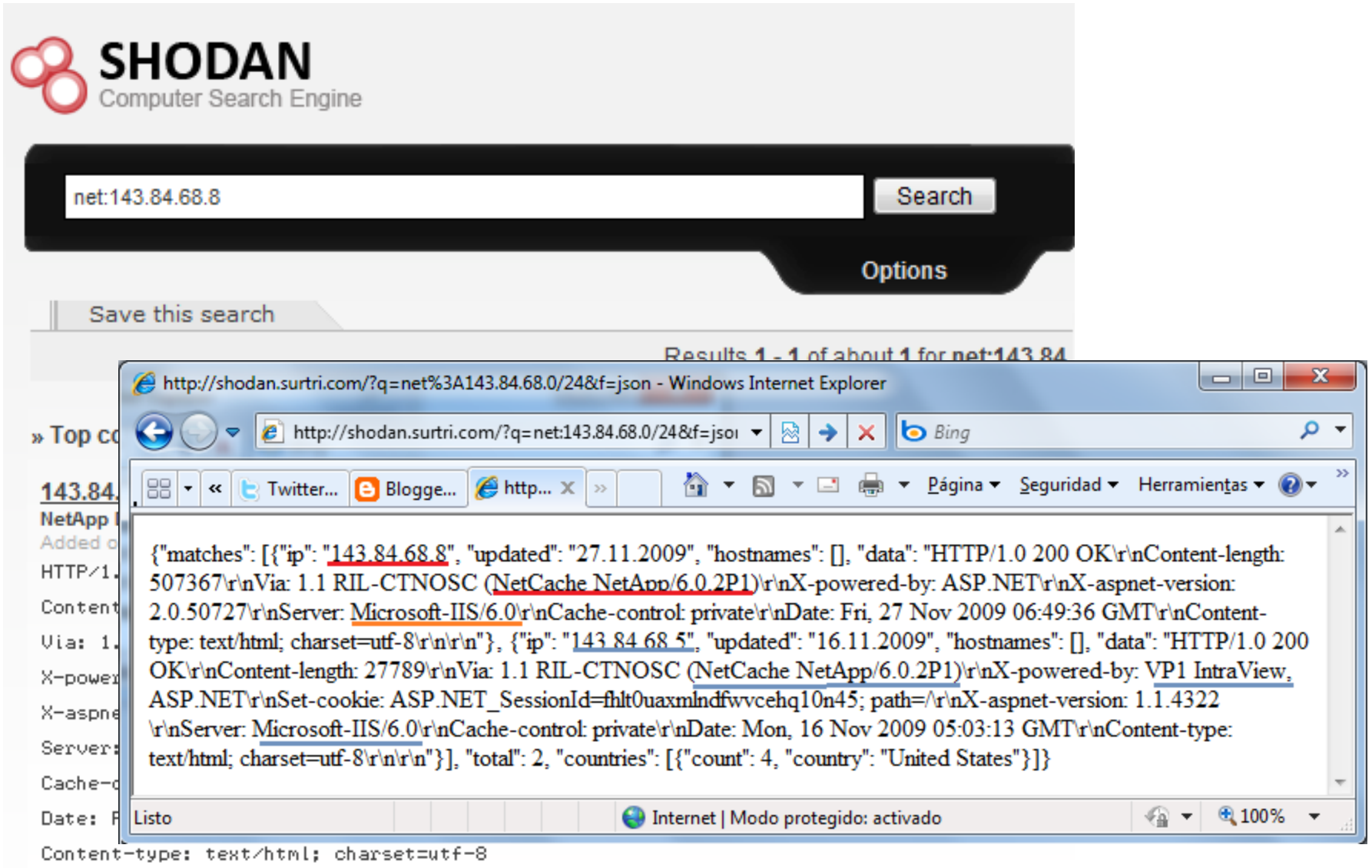
Aplica “algoritmo voraz”
Sigue todos los caminos
Profundidad del algoritmo es configurable
Detecta casi todas las referencias accesibles

```
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:
```

FOCA & SHODAN


SHODAN
Computer Search Engine
net:143.84.68.8
Search
Options
Save this search
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%
Content-type: text/html; charset=utf-8

ALGUNA DEMO CON FOCA 2

FOCA sólo corre en Windows

Evolución: SW recognition

/Rooted 2010

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

Más de 20.000 FOCAs

Chema Alonso
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