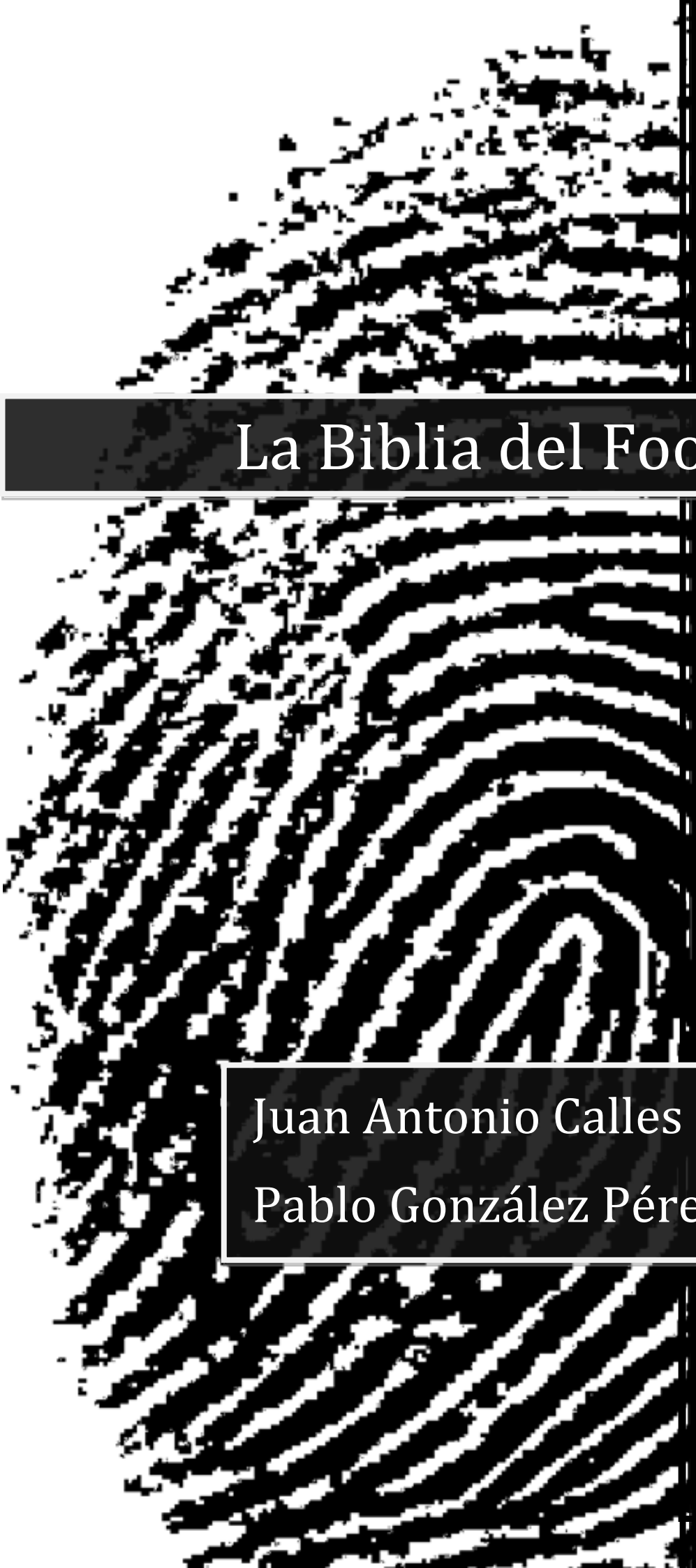


# La Biblia del Footprinting

Juan Antonio Calles García

Pablo González Pérez

Flu Project

2011

## CONTENIDO

## PRÓLOGO

El presente libro pretende servir como manual de auditoría de seguridad informática. Se centra específicamente en la fase de Footprinting, que se corresponde con la primera fase de los procesos de auditoría de Caja Negra y Test de Penetración.

Hemos intentado describir mediante una serie de pasos una posible manera de realizar la búsqueda de información necesaria para las posteriores fases de la auditoría, analizando algunas de las principales herramientas disponibles en el mercado.

El libro será ampliado en futuras versiones con más herramientas y análisis más profundos.

## LA FASE DE FOOTPRINTING

El proceso de Footprinting consiste en la búsqueda de toda la información pública, bien porque haya sido publicada a propósito o bien porque haya sido publicada por desconocimiento (abierta, por tanto no estaremos incurriendo en ningún delito, además la entidad ni debería detectarlo) que pueda haber sobre el sistema que se va a auditar, es decir, buscaremos todas las huellas posibles, como direcciones IP, servidores internos, cuentas de correo de los usuarios, nombres de máquinas, información del registrador del dominio, tipos de servidores, ficheros con cuentas y/o credenciales de usuarios, impresoras, cámaras IP, metadatos, etc. Es decir, cualquier dato que nos pueda ser de utilidad para lanzar distintos ataques en las fases posteriores de la auditoría.

Si enumeramos los pasos más o menos genéricos para realizar un Pentest, el proceso de Footprinting sería el primero de ellos:

1. **Footprinting**.
2. Fingerprinting.
3. Análisis de vulnerabilidades.
4. Explotación de vulnerabilidades.
5. Generación de informes.

Pongamos como ejemplo que tenemos que auditar a la organización Flu Project que tiene en el dominio flu-project.com su sitio Web y desde el que se pueden conectar a distintos servicios que ofrece su organización.

### 1. VISITAR EL SITIO WEB

El primer paso será evidentemente entrar en el sitio Web que vamos a auditar. Deberemos navegar por todas sus páginas y aplicaciones, ya que nunca sabemos que nos vamos a encontrar. Es habitual, sobretodo en sitios Web muy grandes, que se dejen olvidados enlaces a sitios que no deberían estar, o algún error en una llamada a BBDD (algo más común de lo que se piensa). Tras hacernos una idea del estado de la web continuaremos con el siguiente paso.

### 2. ¿QUÉ SABEN LOS BUSCADORES DE NUESTRO OBJETIVO?

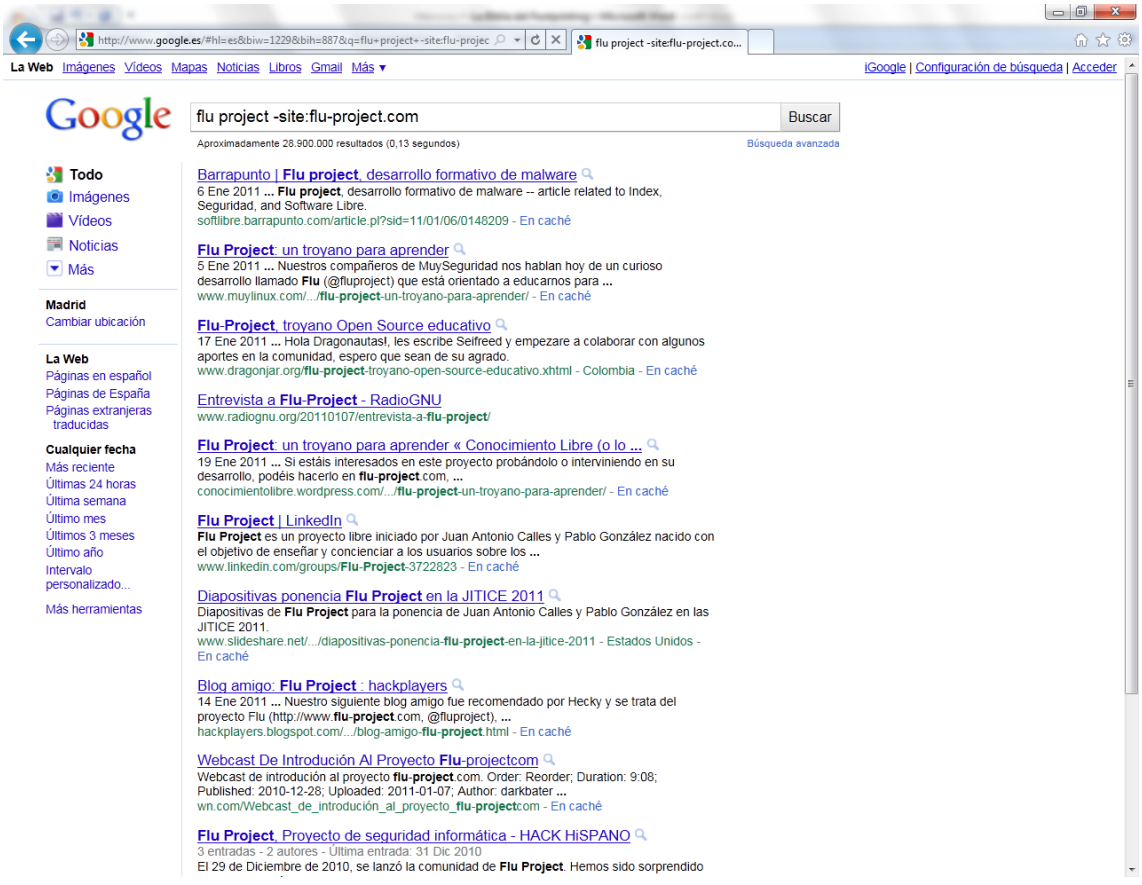
El segundo paso de cualquier proceso de Footprinting sería preguntar a Google, Bing, etc. por el dominio del que queremos obtener información. Lo bueno (o malo según se mire…) de los buscadores es que sus crawlers suelen indexar en

ocasiones ciertas páginas que no deberían haberse publicado pero que han estado cierto tiempo visibles desde Internet mientras se estaban probando, y han quedado cacheadas en Google. Por tanto, podríamos verlas mirando la caché o con algún servicio como "archive.org".

Continuaremos con las búsquedas hacking utilizando diferentes verbos para refinar un poco más las búsquedas. Para el caso de Google Hacking podéis ver los verbos disponibles aquí. Y para el caso de Bing Hacking, aquí.

Por ejemplo, es interesante ver qué saben o dicen los demás de nuestro objetivo, para ello, podemos ayudarnos de la siguiente búsqueda en Google, donde el "–" indica que queremos ver todos los resultados menos los del dominio objetivo:

```
Flu project -site:flu-project.com
```

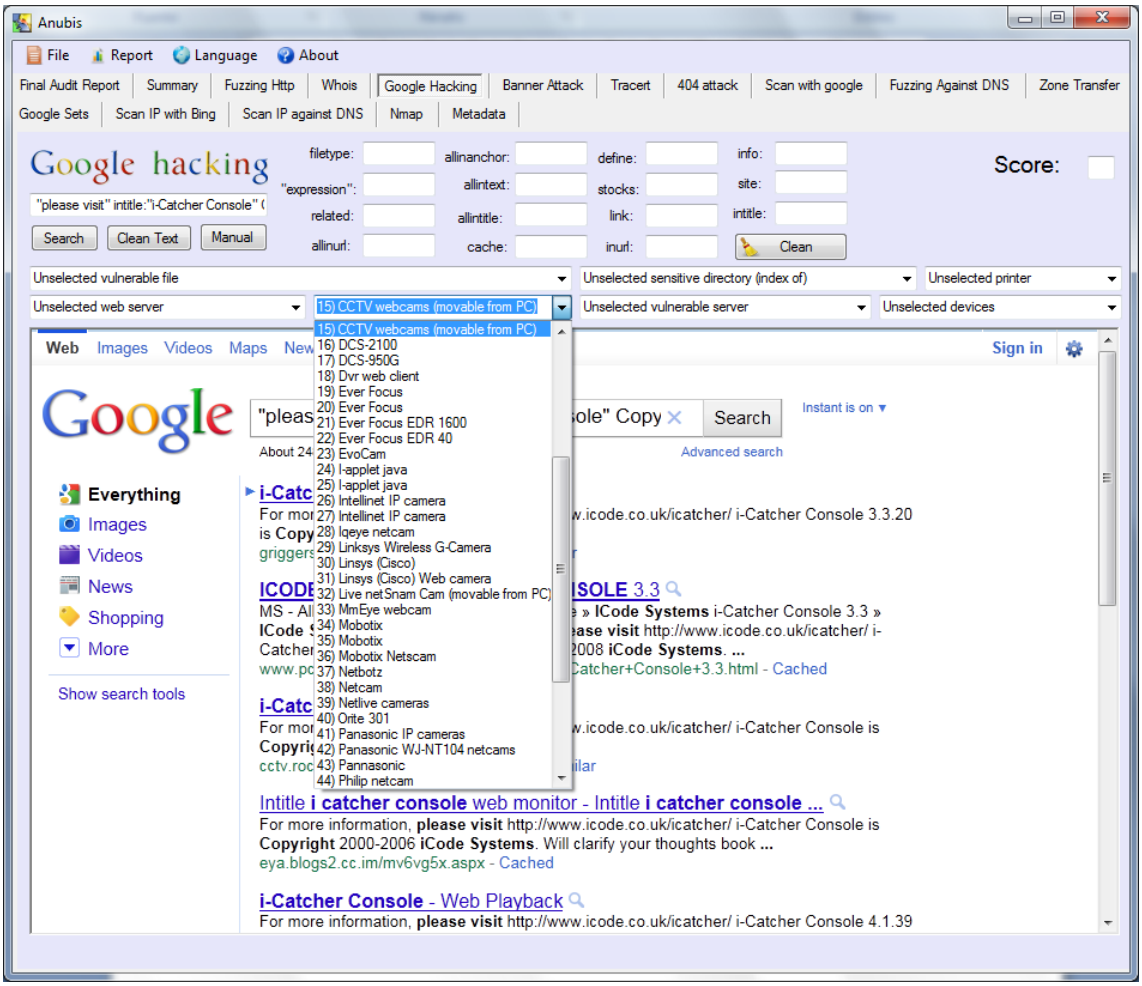



Algunos verbos a destacar serían:

- **site**: para listar toda la información de un dominio concreto.

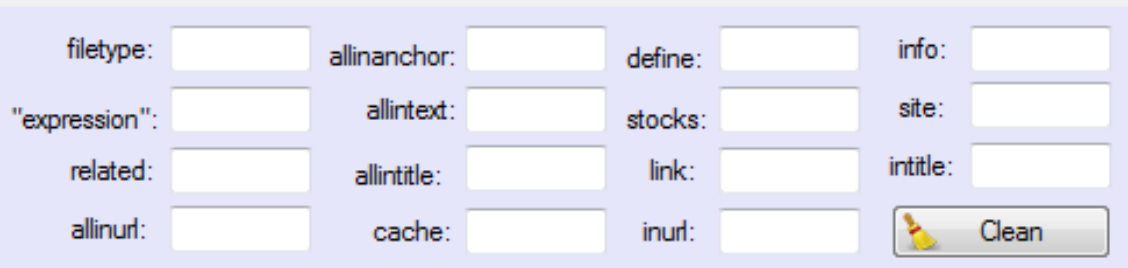
- **filetype o ext**: para buscar archivos de un formato determinado, por ejemplo pdfs, rdp (de escritorio remoto), imágenes png, jpg, etc. para obtener información EXIF y un largo etcétera.
- **intitle**: para buscar páginas con ciertas palabras en el campo title.
- **inurl**: para buscar páginas con ciertas palabras en la URL.
- O buscar por ejemplo por la frase "index of" para encontrar listados de archivos de ftps, etc.

Si queréis estudiar diferentes ejemplos de búsquedas avanzadas podéis pasaros por la Google Hacking Database (GHDB). La GHDB es un repositorio con búsquedas posibles en Google que se pueden utilizar para obtener datos confidenciales de servidores, como ficheros de configuración, nombres, cámaras, impresoras, passwords, etc. La base de datos está algo desactualizada, pero hemos analizado la base de datos entera, y se han predefinido las búsquedas que aún funcionaban y son más interesantes en la herramienta Anubis:



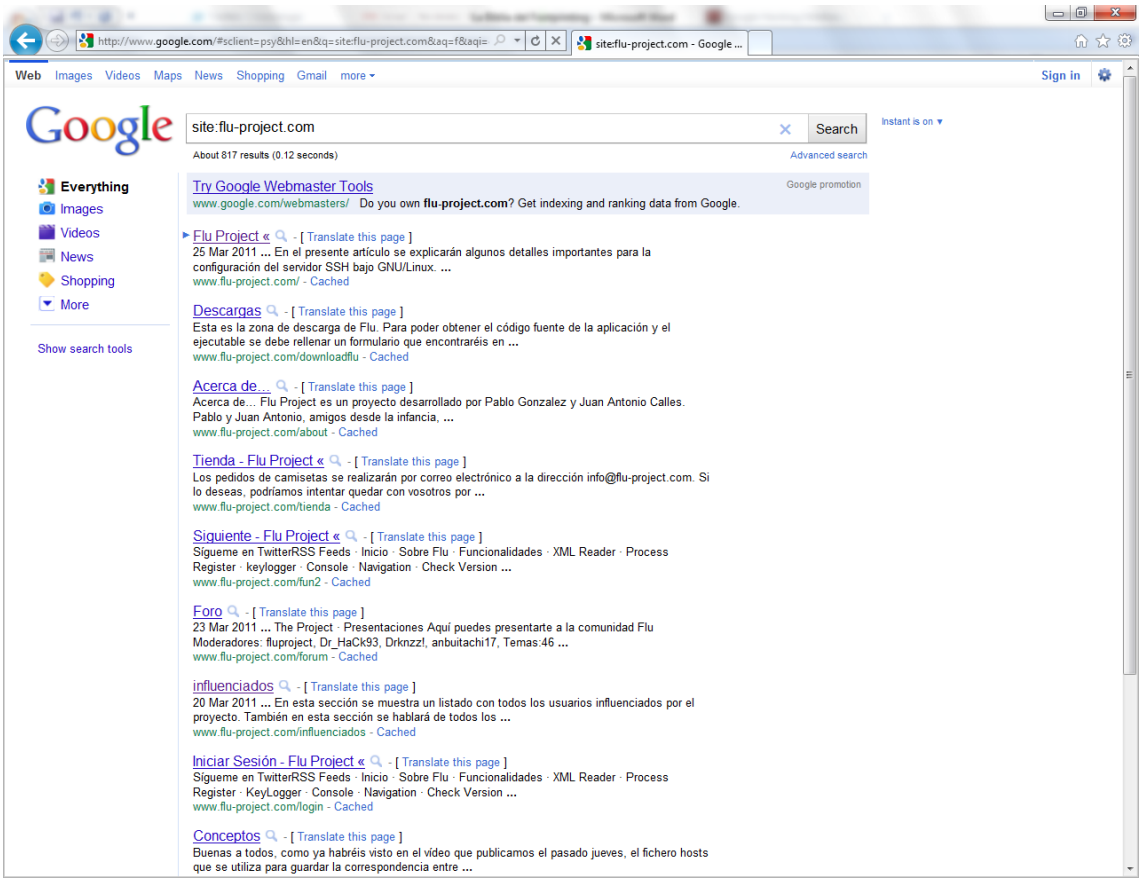

La herramienta la podéis descargar gratuitamente desde el blog personal de Juan Antonio Calles (http://elblogdecalles.blogspot.com). Tenedla a mano porque la utilizaremos a menudo durante este libro.

En esta herramienta también tenéis la posibilidad de indicar los verbos en las casillas en blanco para facilitaros más la tarea:




Una vez que hayamos realizado algunas búsquedas específicas será interesante listar todas las páginas que pendan del dominio raíz. Para ello podemos ayudarnos de la búsqueda:

```
site:flu-project.com
```

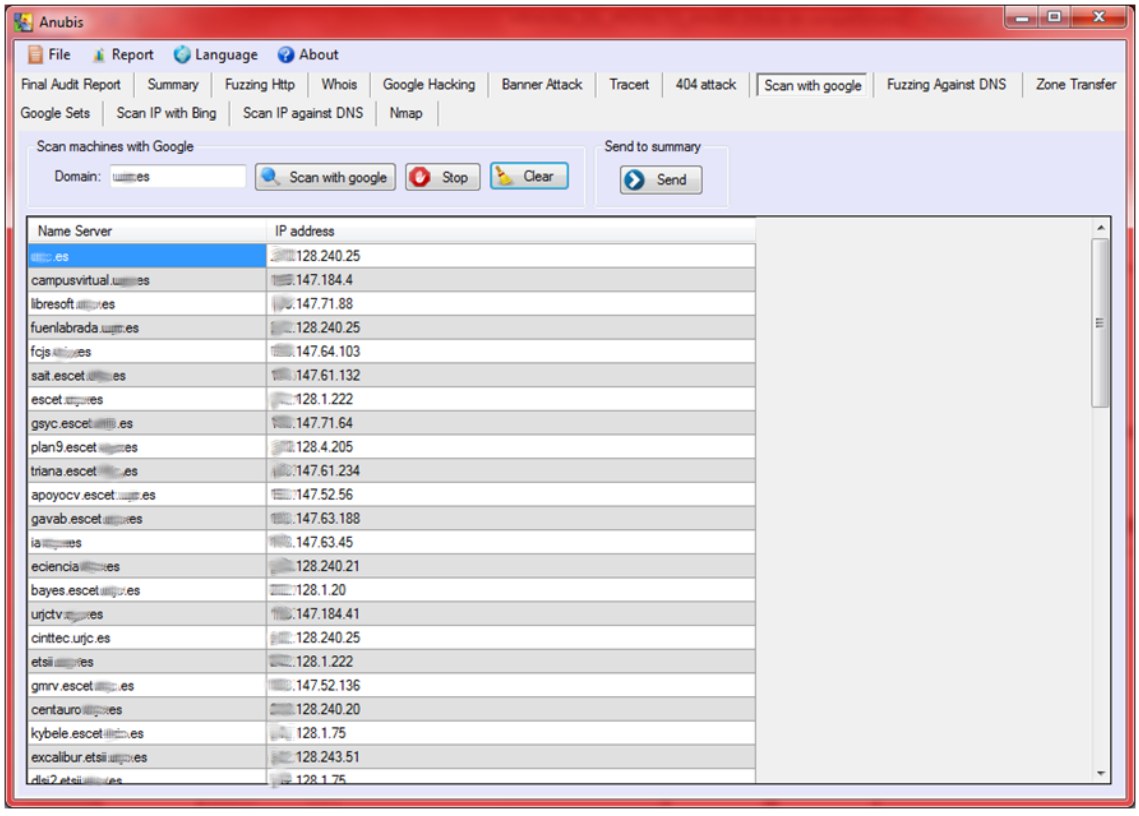



Y podríamos leernos el código fuente de las distintas páginas encontradas, para ver si hay comentarios escritos por los programadores (algo común) u otros datos que puedan ser de utilidad. Por ejemplo, en una ocasión nos encontramos con un comentario muy curioso que decía algo como lo siguiente:

<!—Comentario del Diseñador al Programador, el usuario para conectarse a la BBDD es PEPITO y la clave MENGANITO-->

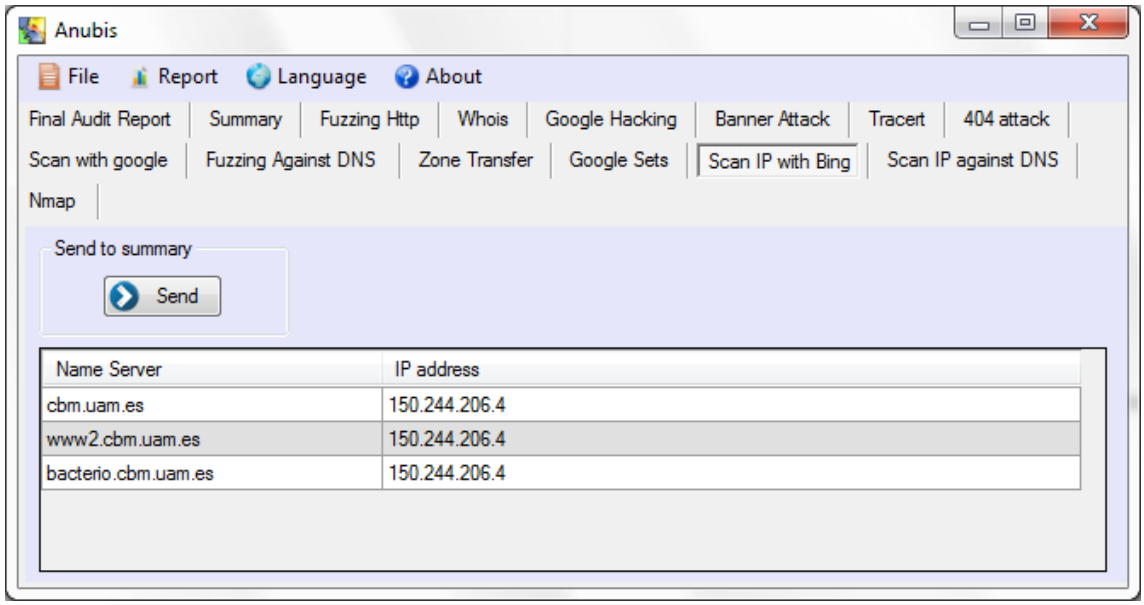
Si queréis trabajar un poco menos podéis descargaros el sitio web entero, con alguna herramienta como Teleport o WebZip y hacer búsquedas directamente sobre la carpeta donde esté el sitio web descargado con la herramienta Inforapid, que realiza búsquedas muy rápidas sobre el contenido de los ficheros de una carpeta.

Otro dato interesante será listar los subdominios que pendan del dominio principal con sus correspondientes direcciones IP y, por tanto, máquinas y servidores. De esta manera, nos podremos dar cuenta rápidamente del tamaño de la organización. Para ello, nos podremos ayudar de nuevo de la herramienta Anubis que automatiza búsquedas de Google Hacking con los verbos "site" e "inurl". Con estos datos posteriormente en la fase de Fingerprinting (activo), con Nmap por ejemplo, podremos intentar obtener más datos y en fases posteriores realizar otro tipo de ataques:




También podremos encontrarnos con que varios dominios compartan una IP (virtual hosts), con lo que para buscarlos nos será de especial utilidad el buscador Bing con su verbo "IP":


Anubis lleva integrada también esta búsqueda y, como veis, se obtienen los mismos resultados, solo que ya filtrados, eliminando los resultados repetidos:

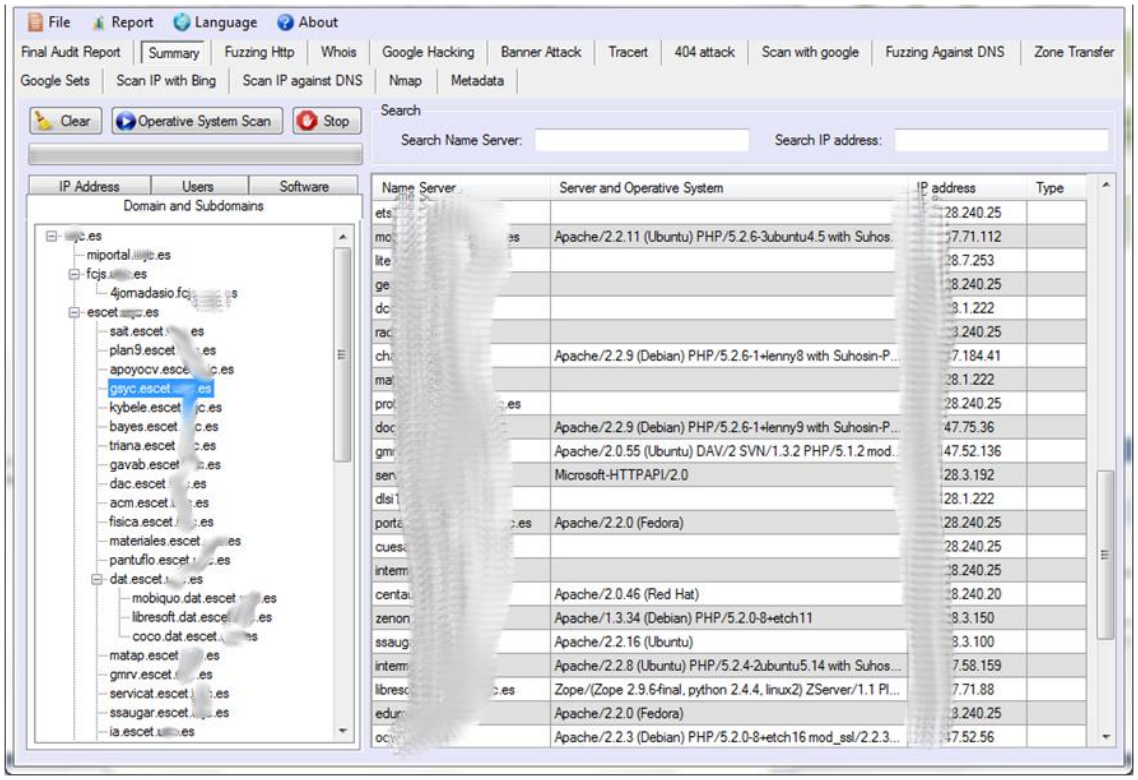


Para esta tarea podéis utilizar también algún servicio Web como los siguientes:

http://serversniff.net/content.php?do=hostonip


http://www.myipneighbors.com/

Todos estos datos deberíamos irlos enumerando de una manera adecuada y permitiendo cierta trazabilidad entre los distintos elementos que vayamos encontrando, esta tarea es todo un arte, y es algo que han tenido presente los desarrolladores de algunas herramientas como Maltego, OPTOS, Foca, y Anubis. De esta última podéis ver una captura a continuación:

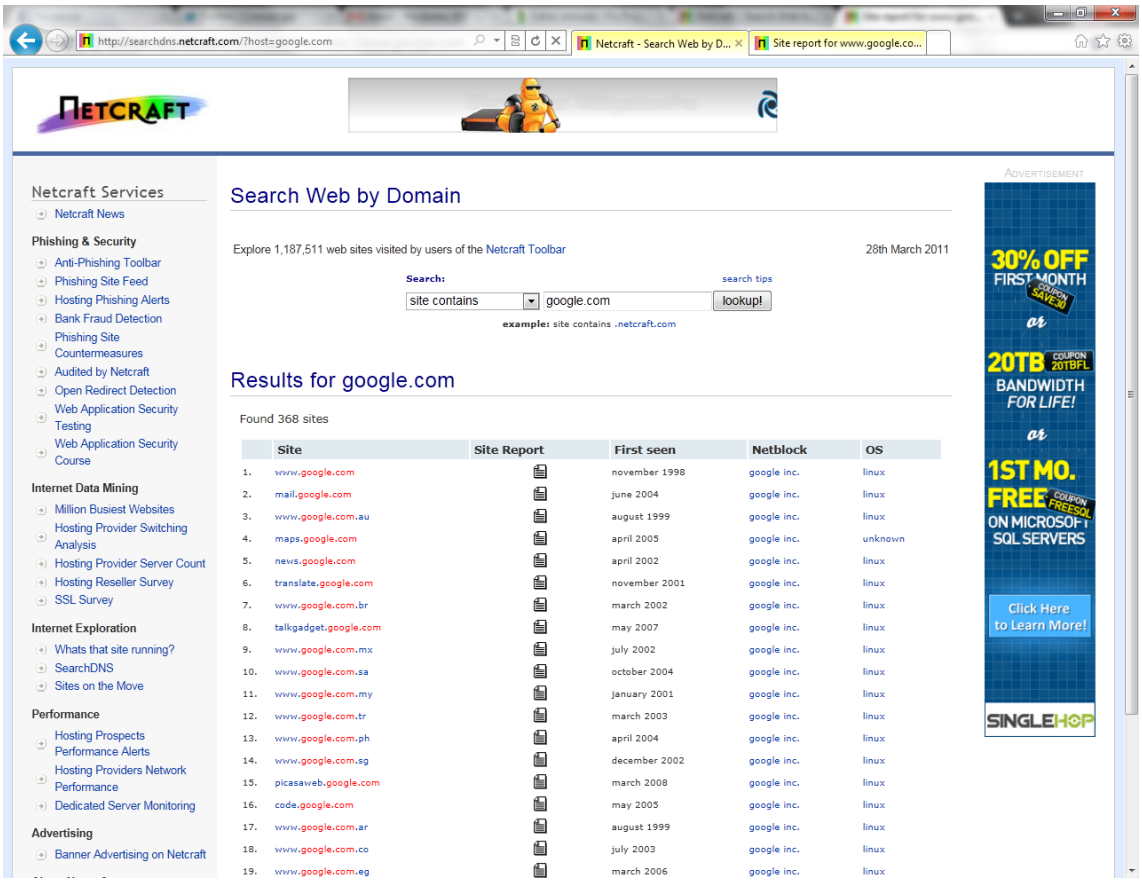


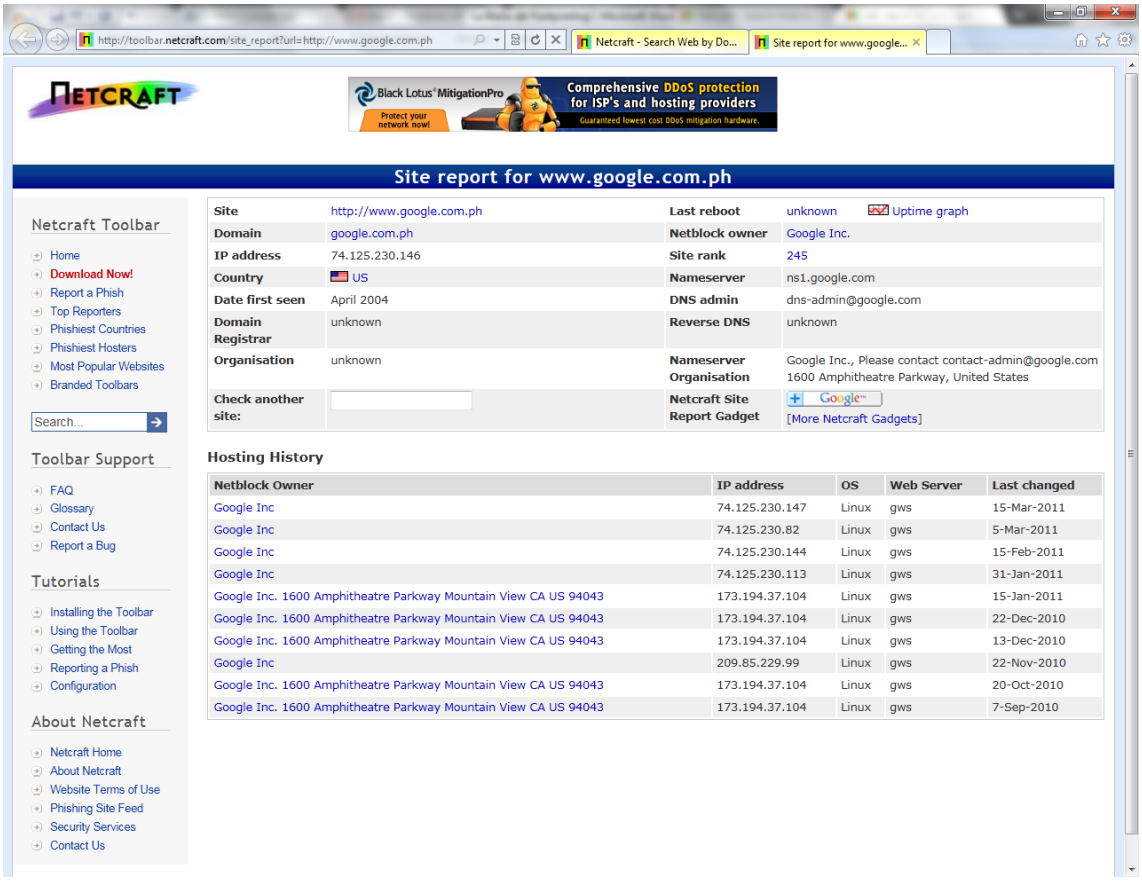

## 3. SERVICIOS WEB DE BÚSQUEDA DE INFORMACIÓN DE UN DOMINIO

El tercer paso que vamos a seguir en la búsqueda de información será el uso de distintos servicios Web que hay por Internet y que nos permitirán analizar ciertos datos del dominio objetivo como por ejemplo su dirección IP, los subdominios que cuelgan del dominio principal, su registrador mediante consultas Whois, su localización en mapas, trazas, servidores de DNS, etc.

**Netcraft (http://searchdns.netcraft.com)**

Este servicio nos permitirá analizar los subdominios de un determinado dominio, proporcionándonos datos como sus direcciones IP, Servidores Web, Sistemas Operativos, etc.

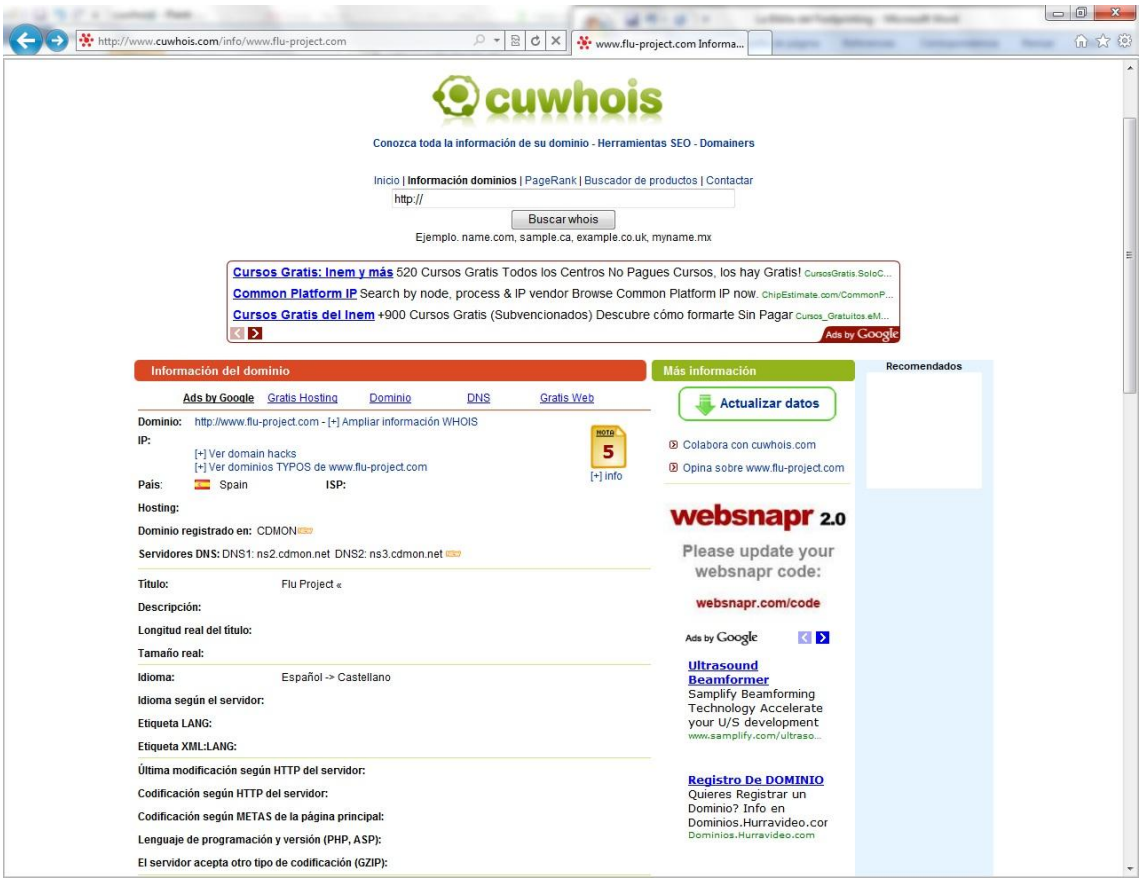

http://searchdns.netcraft.com/?host=google.com
Netcraft - Search Web by D...
Site report for www.google.co...
NETCRAFT
Netcraft Services
Netcraft News
Phishing & Security
Anti-Phishing Toolbar
Phishing Site Feed
Hosting Phishing Alerts
Bank Fraud Detection
Phishing Site Countermeasures
Audited by Netcraft
Open Redirect Detection
Web Application Security Testing
Web Application Security Course
Internet Data Mining
Million Busiest Websites
Hosting Provider Switching Analysis
Hosting Provider Server Count
Hosting Reseller Survey
SSL Survey
Internet Exploration
Whats that site running?
SearchDNS
Sites on the Move
Performance
Hosting Prospects Performance Alerts
Hosting Providers Network Performance
Dedicated Server Monitoring
Advertising
Banner Advertising on Netcraft
Search Web by Domain
Explore 1,187,511 web sites visited by users of the Netcraft Toolbar
28th March 2011
Search:
search tips
site contains
google.com
lookup!
example: site contains .netcraft.com
Results for google.com
Found 368 sites
Site
Site Report
First seen
Netblock
OS
1. www.google.com november 1998 google inc. linux
2. mail.google.com june 2004 google inc. linux
3. www.google.com.au august 1999 google inc. linux
4. maps.google.com april 2005 google inc. unknown
5. news.google.com april 2002 google inc. linux
6. translate.google.com november 2001 google inc. linux
7. www.google.com.br march 2002 google inc. linux
8. talkgadget.google.com may 2007 google inc. linux
9. www.google.com.mx july 2002 google inc. linux
10. www.google.com.sa october 2004 google inc. linux
11. www.google.com.my january 2001 google inc. linux
12. www.google.com.tr march 2003 google inc. linux
13. www.google.com.ph april 2004 google inc. linux
14. www.google.com.sg december 2002 google inc. linux
15. picasaweb.google.com march 2008 google inc. linux
16. code.google.com may 2005 google inc. linux
17. www.google.com.ar august 1999 google inc. linux
18. www.google.com.co july 2003 google inc. linux
19. www.google.com.eg march 2006 google inc. linux
ADVERTISEMENT
30% OFF FIRST MONTH
or
20TB BANDWIDTH FOR LIFE!
or
1ST MO. FREE ON MICROSOFT SQL SERVERS
Click Here to Learn More!
SINGLEHOP


http://toolbar.netcraft.com/site_report?url=http://www.google.com.ph
Netcraft - Search Web by Do...
Site report for www.google...
NETCRAFT
Black Lotus MitigationPro
Protect your network now!
Comprehensive DDoS protection for ISP's and hosting providers
Guaranteed lowest cost DDoS mitigation hardware.
Site report for www.google.com.ph
Netcraft Toolbar
Home
Download Now!
Report a Phish
Top Reporters
Phishiest Countries
Phishiest Hosters
Most Popular Websites
Branded Toolbars
Search...
Toolbar Support
FAQ
Glossary
Contact Us
Report a Bug
Tutorials
Installing the Toolbar
Using the Toolbar
Getting the Most
Reporting a Phish
Configuration
About Netcraft
Netcraft Home
About Netcraft
Website Terms of Use
Phishing Site Feed
Security Services
Contact Us
Site http://www.google.com.ph
Last reboot unknown Uptime graph
Domain google.com.ph
Netblock owner Google Inc.
IP address 74.125.230.146
Site rank 245
Country US
Nameserver ns1.google.com
Date first seen April 2004
DNS admin dns-admin@google.com
Domain Registrar unknown
Reverse DNS unknown
Organisation unknown
Nameserver Organisation Google Inc., Please contact contact-admin@google.com 1600 Amphitheatre Parkway, United States
Check another site:
Netcraft Site Report Gadget
[More Netcraft Gadgets]
Hosting History
Netblock Owner
IP address
OS
Web Server
Last changed
Google Inc 74.125.230.147 Linux gws 15-Mar-2011
Google Inc 74.125.230.82 Linux gws 5-Mar-2011
Google Inc 74.125.230.144 Linux gws 15-Feb-2011
Google Inc 74.125.230.113 Linux gws 31-Jan-2011
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043 173.194.37.104 Linux gws 15-Jan-2011
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043 173.194.37.104 Linux gws 22-Dec-2010
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043 173.194.37.104 Linux gws 13-Dec-2010
Google Inc 209.85.229.99 Linux gws 22-Nov-2010
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043 173.194.37.104 Linux gws 20-Oct-2010
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043 173.194.37.104 Linux gws 7-Sep-2010

**Cuwhois (http://www.cuwhois.com/)**

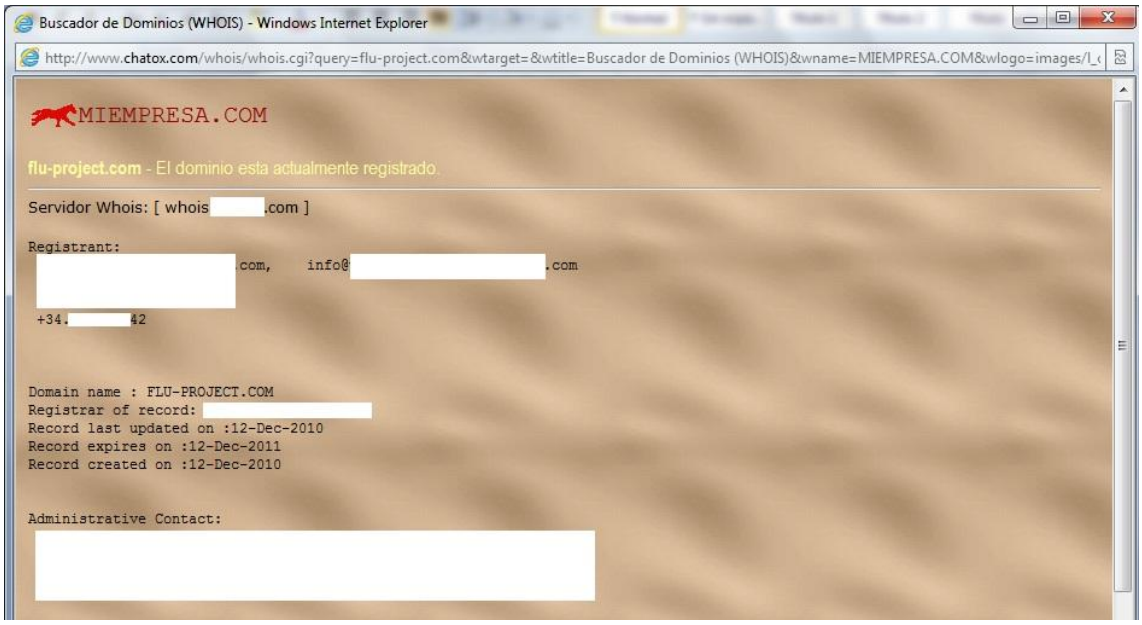
Una auténtica navaja suiza. En la parte superior de la página tenéis enlazadas todas las herramientas que incorpora:


Entre los datos más interesantes que nos podrá aportar se encuentran la IP, Servidores DNS, Registrador del dominio, País, Idioma, Lenguaje de programación del sitio Web, codificación, modelo del Servidor Web, la posición en distintos rankings, feeds, incluso si comparte servidor Web con otras páginas nos proporcionará un listado con sus vecinos:



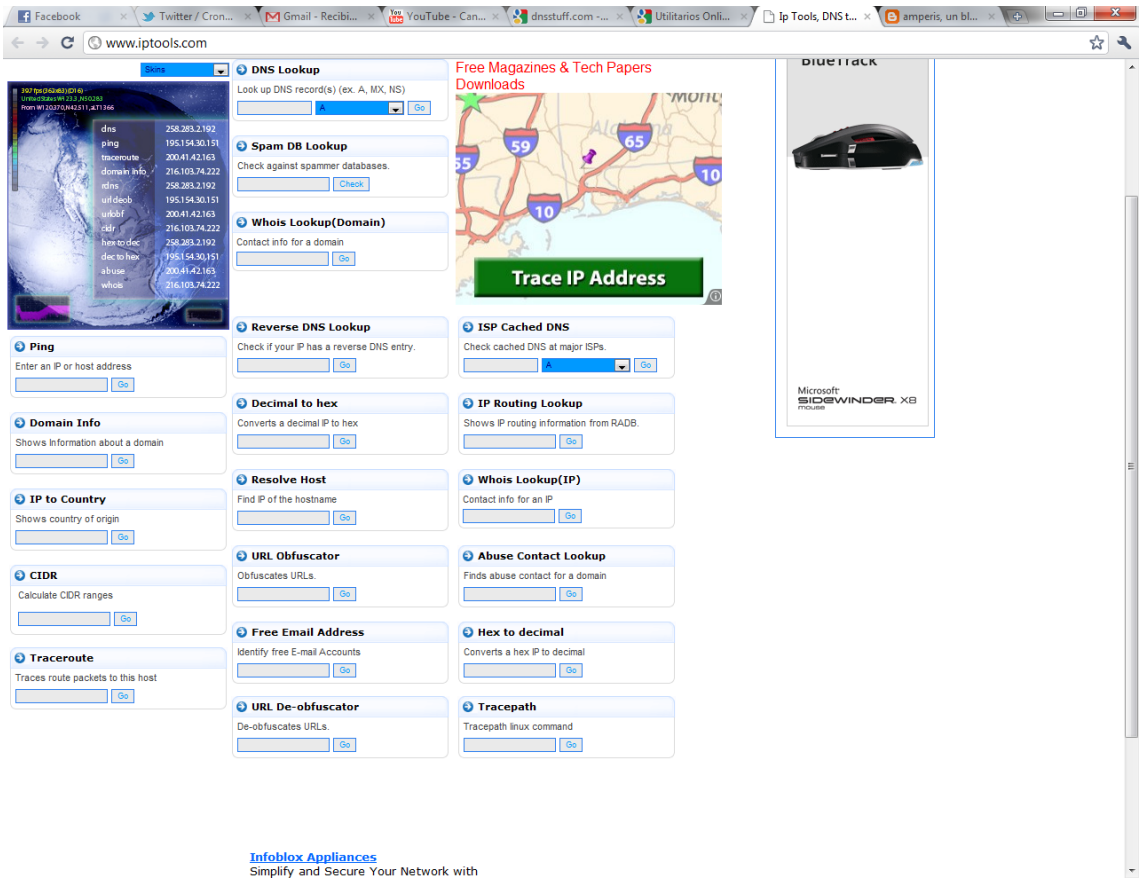

**Chatox (http://www.chatox.com/whois/whois.html)**

Nos proporcionará información del registrador de dominio:




**IPTools (http://www.iptools.com/)**

Es otro servicio Web parecido a Cuwhois que incorpora gran cantidad de herramientas:

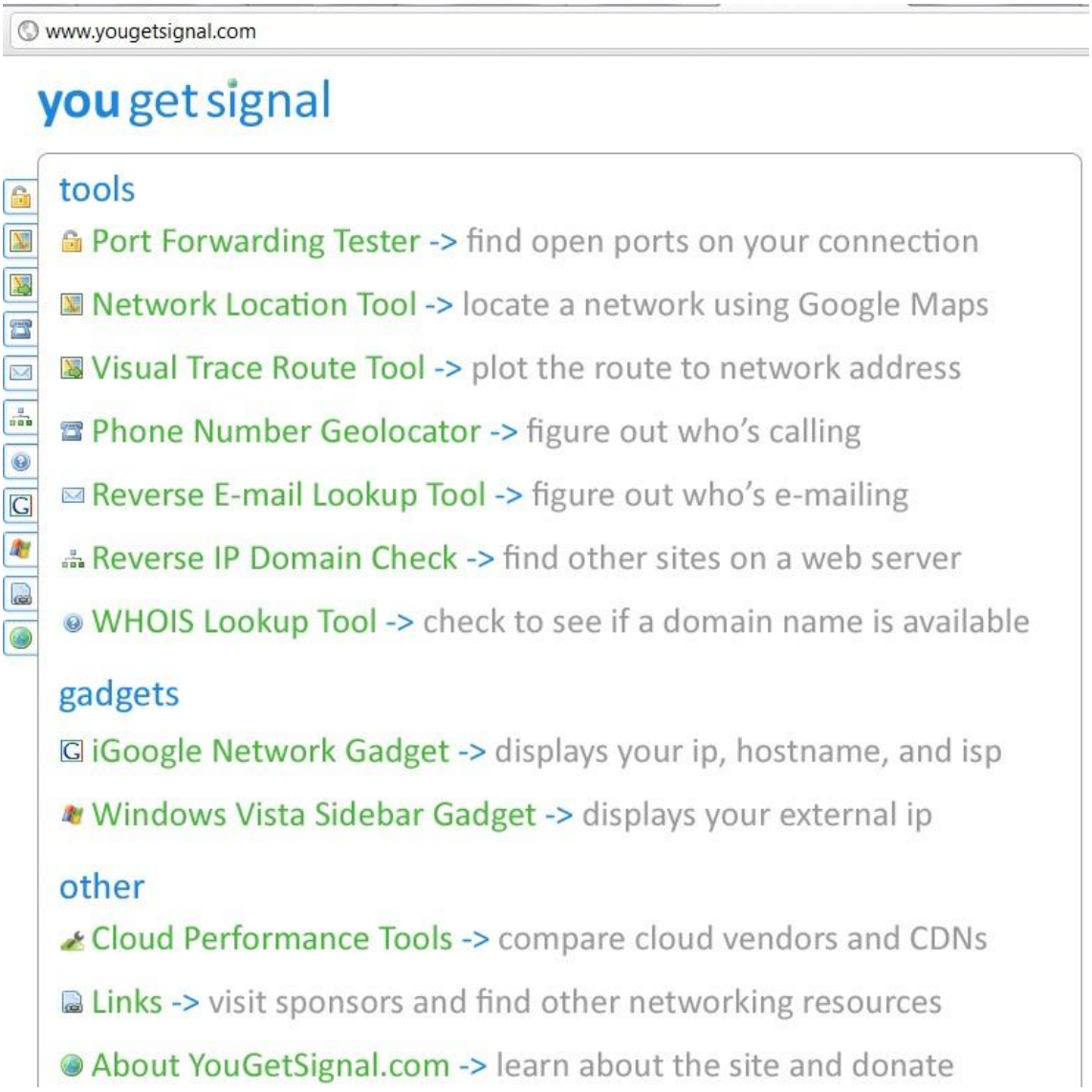



**Robtex (http://www.robtex.com/)**

Otro servicio parecido a Cuwhois, muy completo, que cuenta también con una gran cantidad de herramientas:

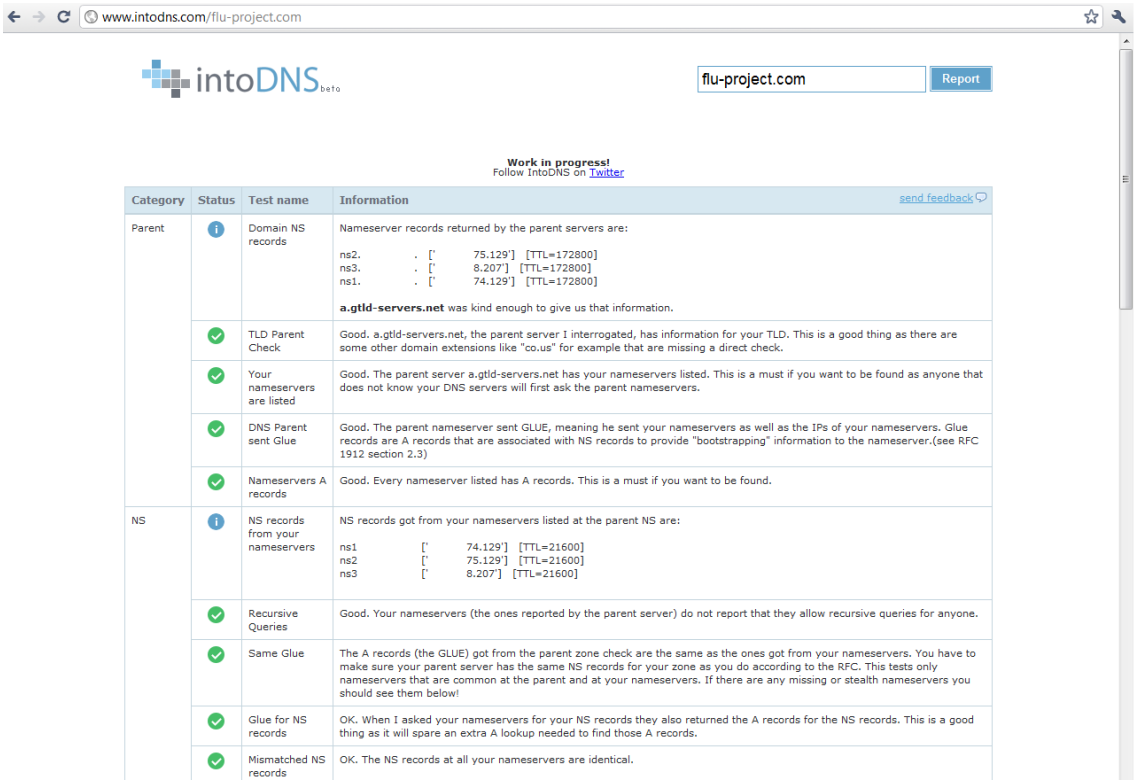
**Yougetsignal (http://www.yougetsignal.com/)**

Otro todo en uno como Cuwhois, Robtex, etc.:



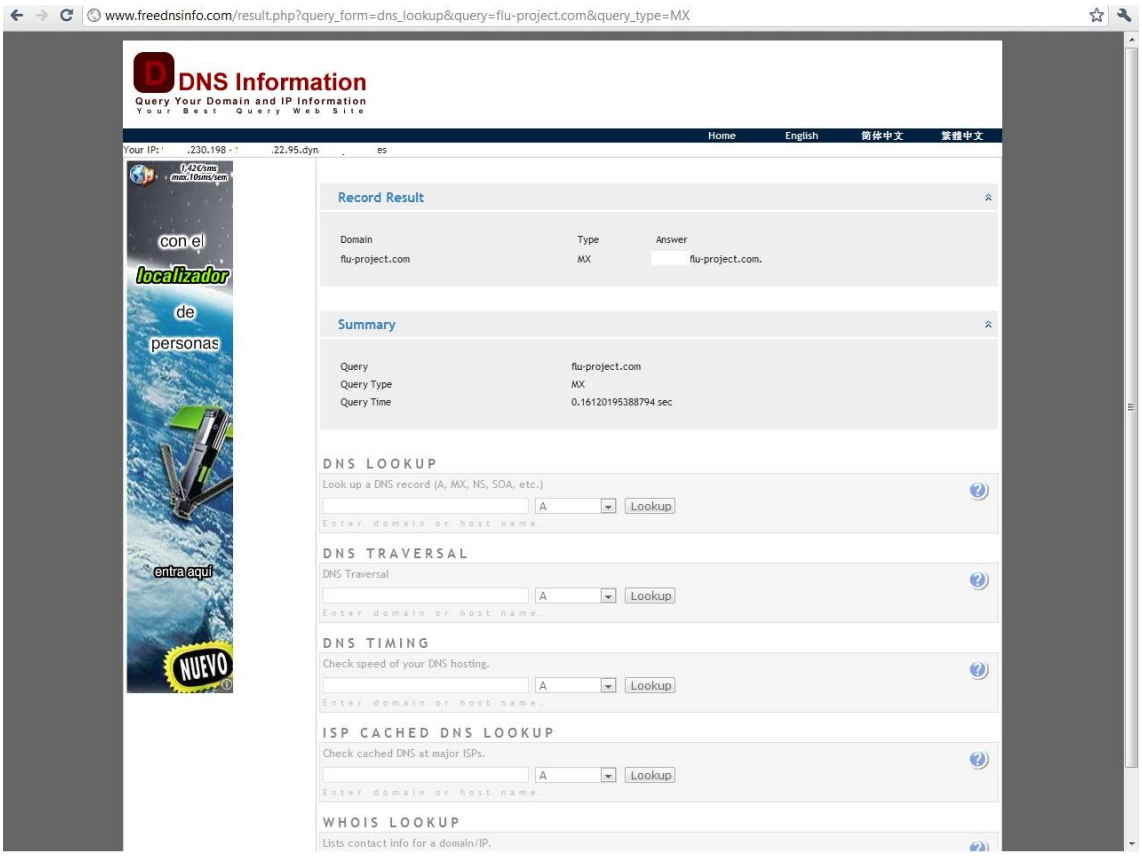

**Intodns (http://www.intodns.com/)**

Herramienta parecida a Cuwhois, Robtex, etc. Permite obtener información de un dominio, IP, servidores de DNS, etc.




**Freednsinfo (http://www.freednsinfo.com/)**

Otra herramientä semejante a IPTools:

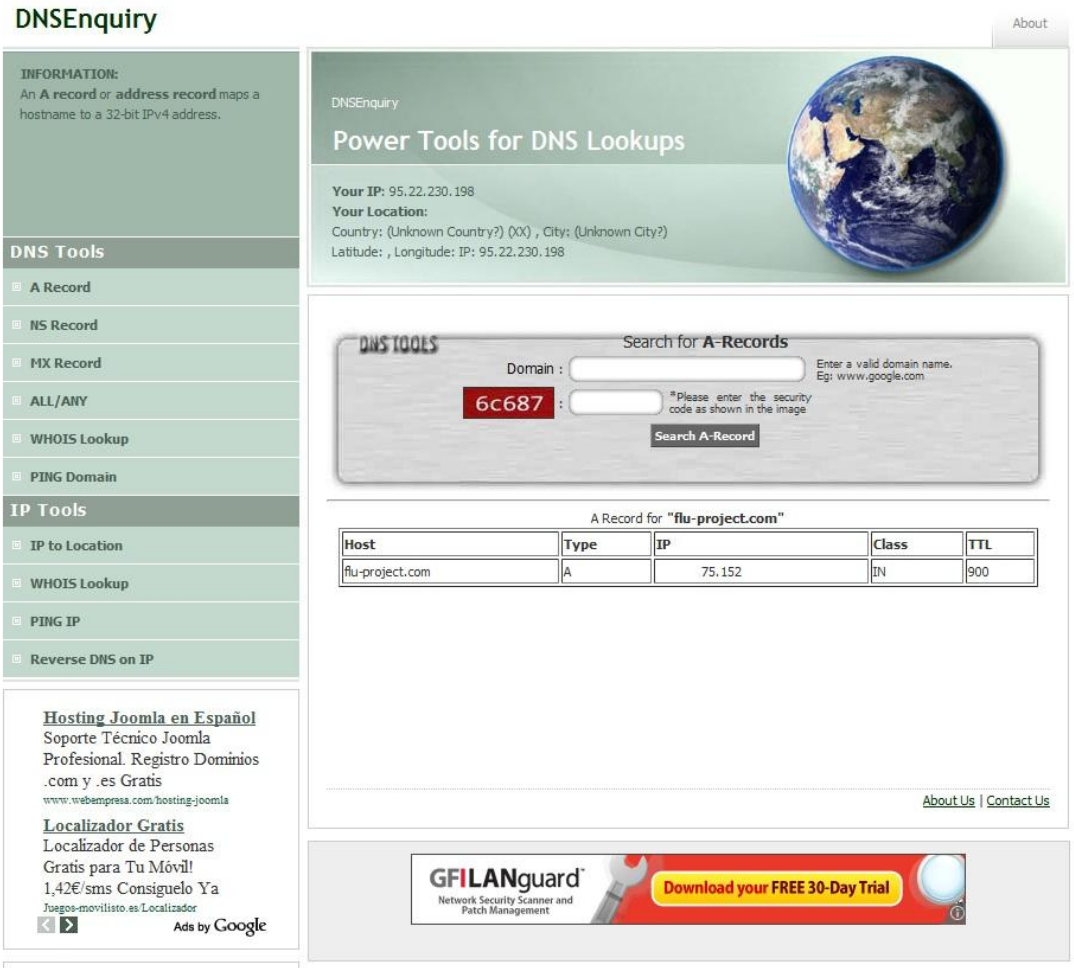


**Dnsstuff (http://www.dnsstuff.com)**

Es un servicio similar a los anteriores, aunque tiene un pero ya que es de pago.

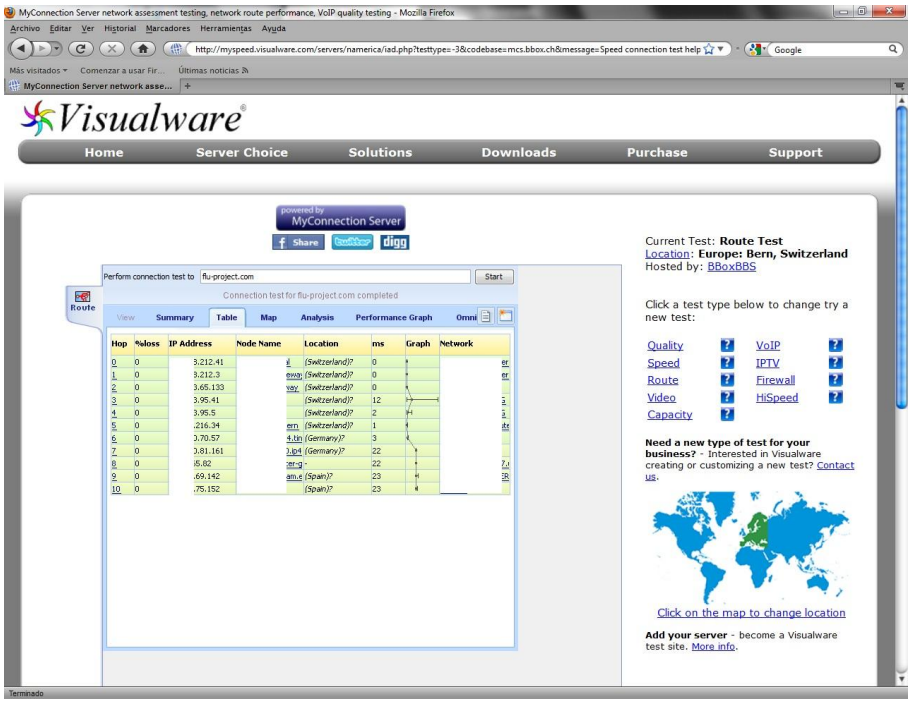
**DnsQuirty (http://www.dnsenquiry.com/)**

Otro servicio que nos permitirá analizar el whois, dns lookup y ping.



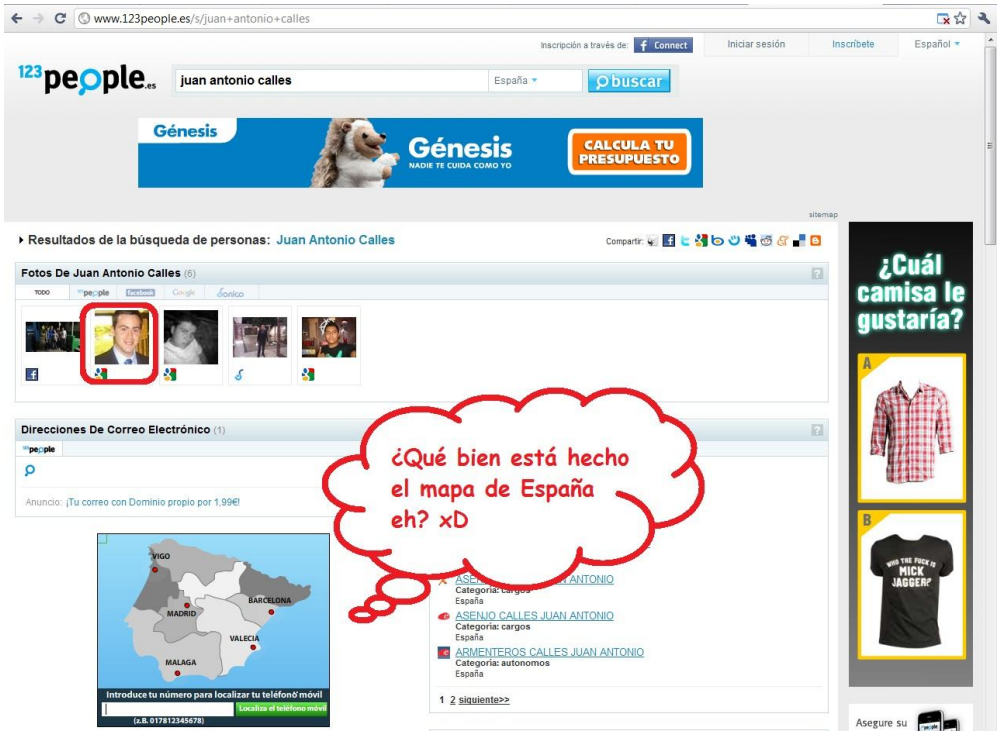

**Visualware**

Servicio Web que nos permitirá seguir visualmente el camino que se recorre hasta llegar a la IP del servidor objetivo. Requiere Java:




**123people (http://www.123people.es/)**

Con éste servicio podremos buscar información sobre personas a partir de su nombre, nos será de utilidad para saber información de una persona cuando hayamos conseguido su nombre a través de metadatos, registro Whois, etc. Nos ayudará a encontrar sus posibles blogs, vídeos subidos a youtube, publicaciones, etc. Analizaremos un poco de su vida para futuros ataques de ingeniería social:



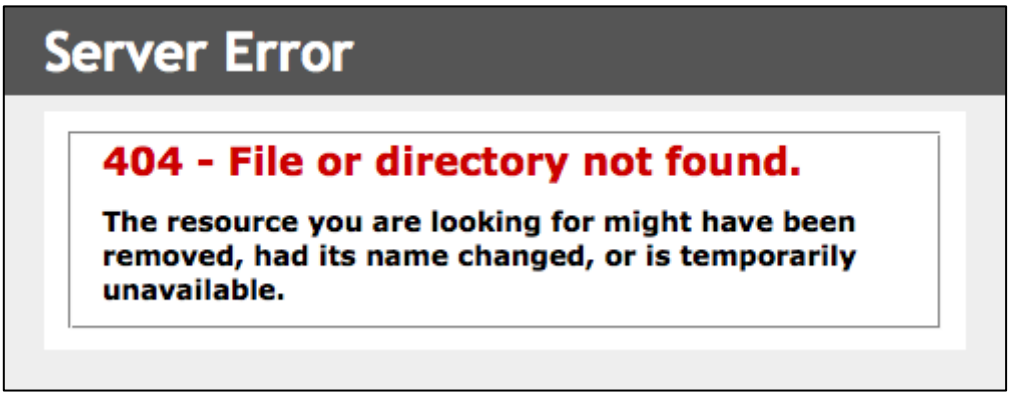
## 4. BÚSQUEDA DE LOS SISTEMAS OPERATIVOS Y MODELOS DE SERVIDOR WEB

Aunque cada vez ocurre menos, todavía numerosos webmasters se olvidan de filtrar o personalizar los errores 404. Recordemos que este error se produce cuando se intenta consultar una página web que no existe en el servidor Web, y si no ha sido modificada, mostrará la página de error por defecto, y que dependiendo del tipo de servidor Web nos podrá dar información del mismo y del sistema operativo.

Nos aprovecharemos de estos errores, consultando páginas web inexistentes para forzar a que el servidor Web nos muestre la información que os acabo de comentar.

Por ejemplo, si consultamos por la página www.XXXXXXXXX.com/asdf veremos la página de error de un Apache 1.3.27 (¡a buscar un exploit! :P):


Si consultamos esta otra página www.YYYYYYYYYY.com/asdf veremos la página de error de un IIS7 y probablemente haya detrás un Microsoft Server 2008, 2008 R2 o un Vista/7:




O si consultamos esta otra página www.ZZZZZZZZZZ.com/asdf veremos la página de error de un IIS6 y probablemente haya detrás un Microsoft Server 2003 o XP:

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

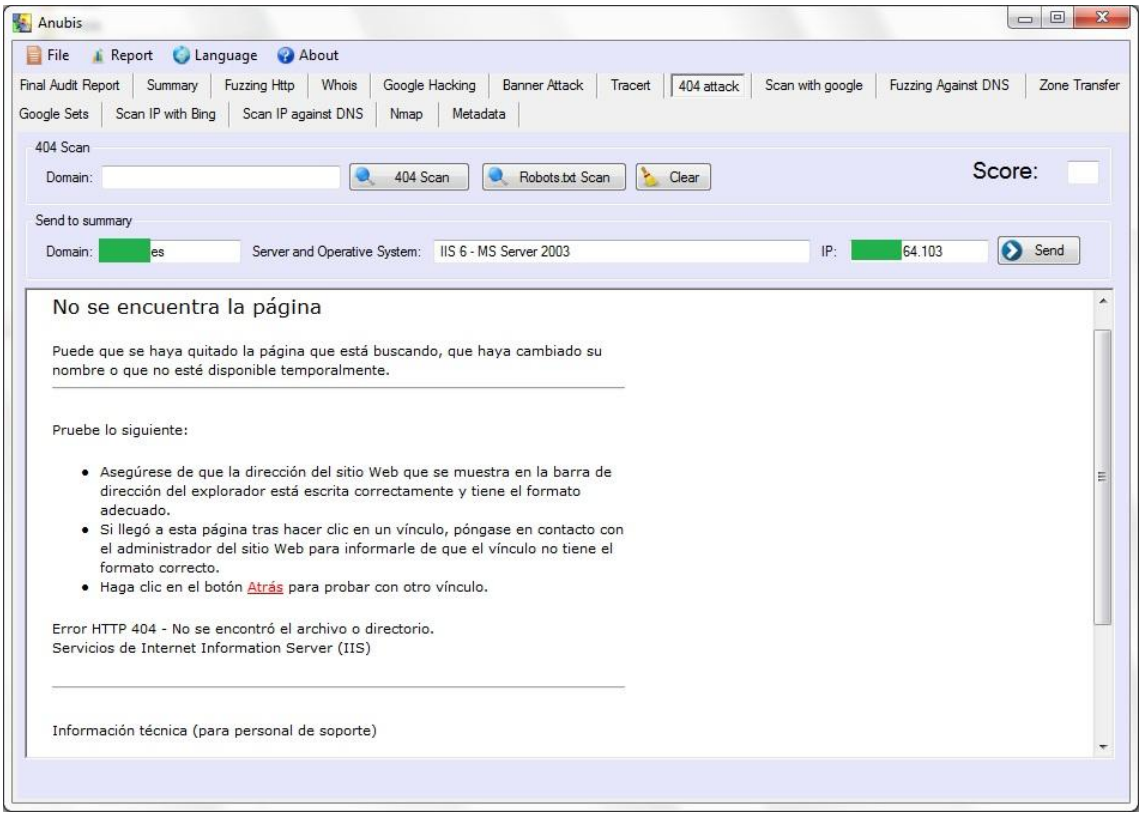
- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **404**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Web Site Setup**, **Common Administrative Tasks**, and **About Custom Error Messages**.

En la herramienta Anubis podéis encontrar una automatización de esta técnica:




Será de utilidad conocer los modelos de servidor web más comunes. Puede ocurrir que algún webmaster nos intente engañar, colocando por ejemplo en un

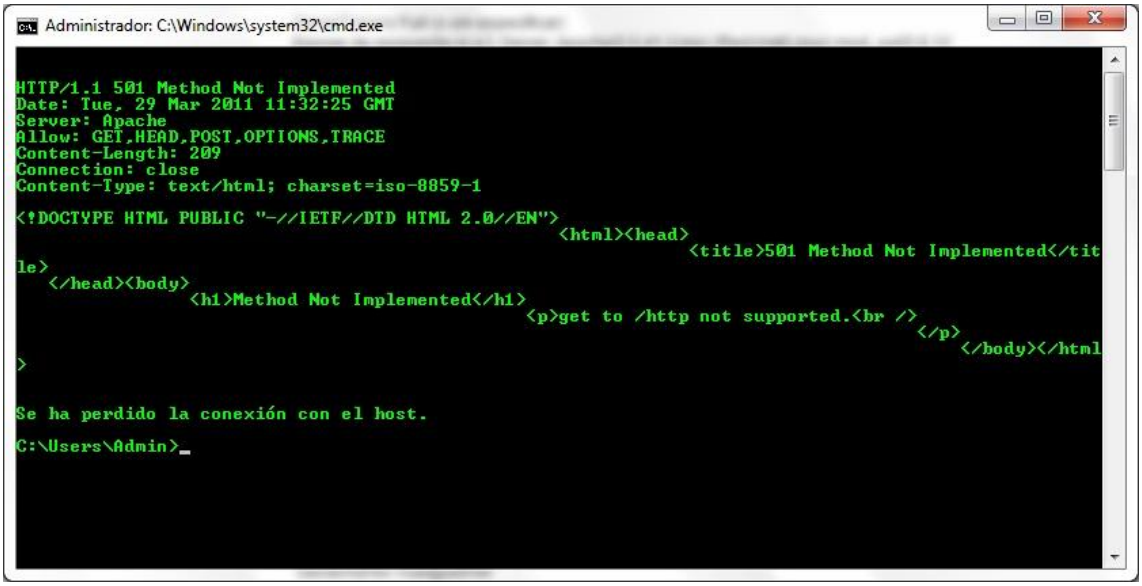
IIS6 una página de error falsa de Apache, por lo que será necesario contrastar la información, por ejemplo, consultando el banner del servidor Web.

Para ello podremos hacerlo desde un CMD en Windows, conectándonos por telnet al puerto 80:


Una vez que se queda la pantalla negra, inyectaremos la siguiente query:

```
get /http /1.0
```

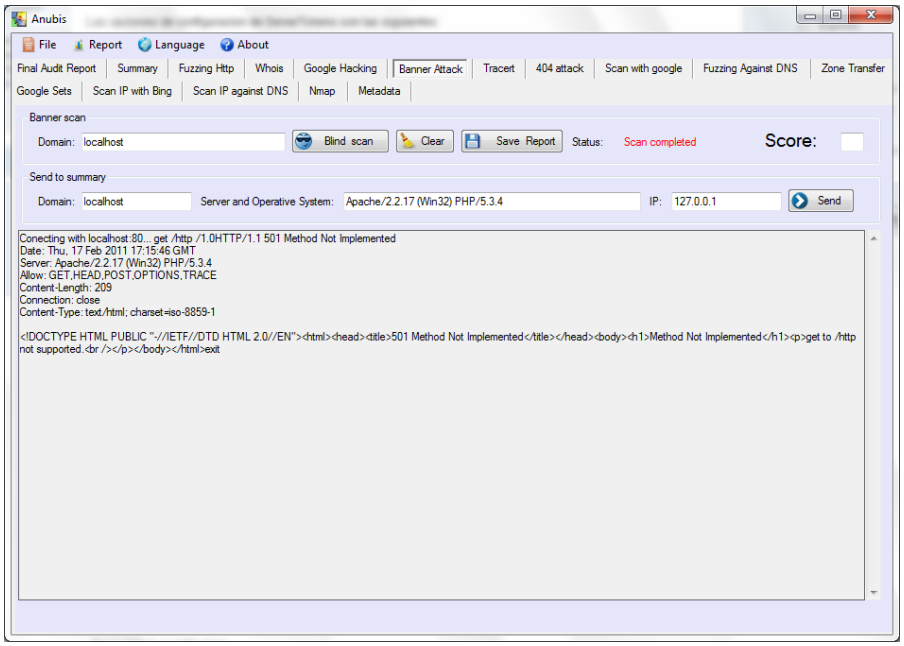
E inmediatamente después pulsaremos algunos “enter”:



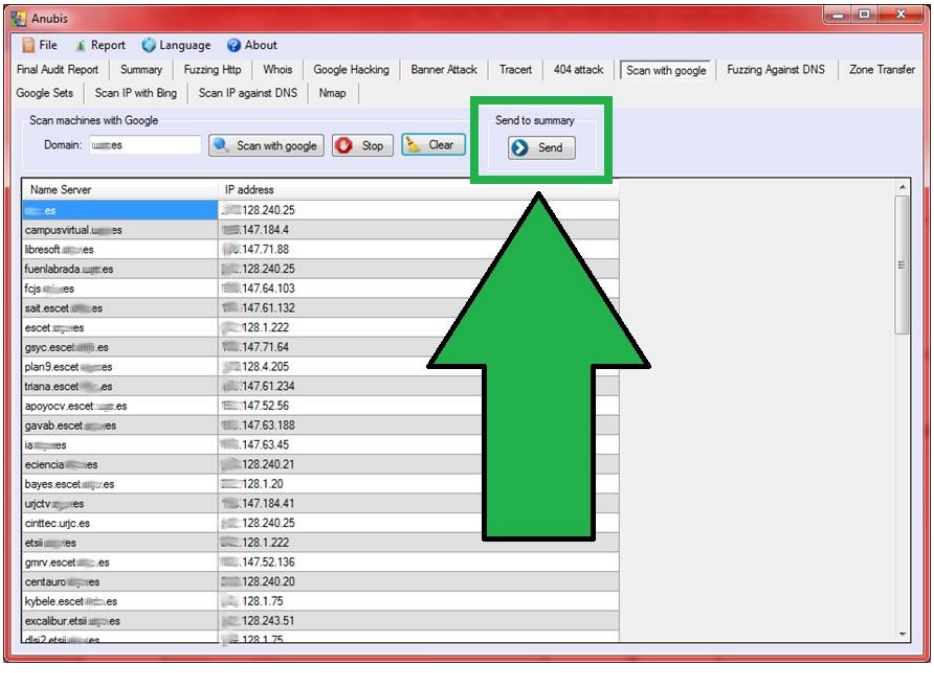

Como veis nos ha mostrado simplemente que se trata de un Apache, no nos ha mostrado nada más porque para el post que hice hace algunas semanas sobre seguridad en los banner, modifiqué el banner reduciendo la cantidad de información mostrada.

En caso de no querer utilizar el CMD, podéis utilizar por ejemplo el cliente Putty.

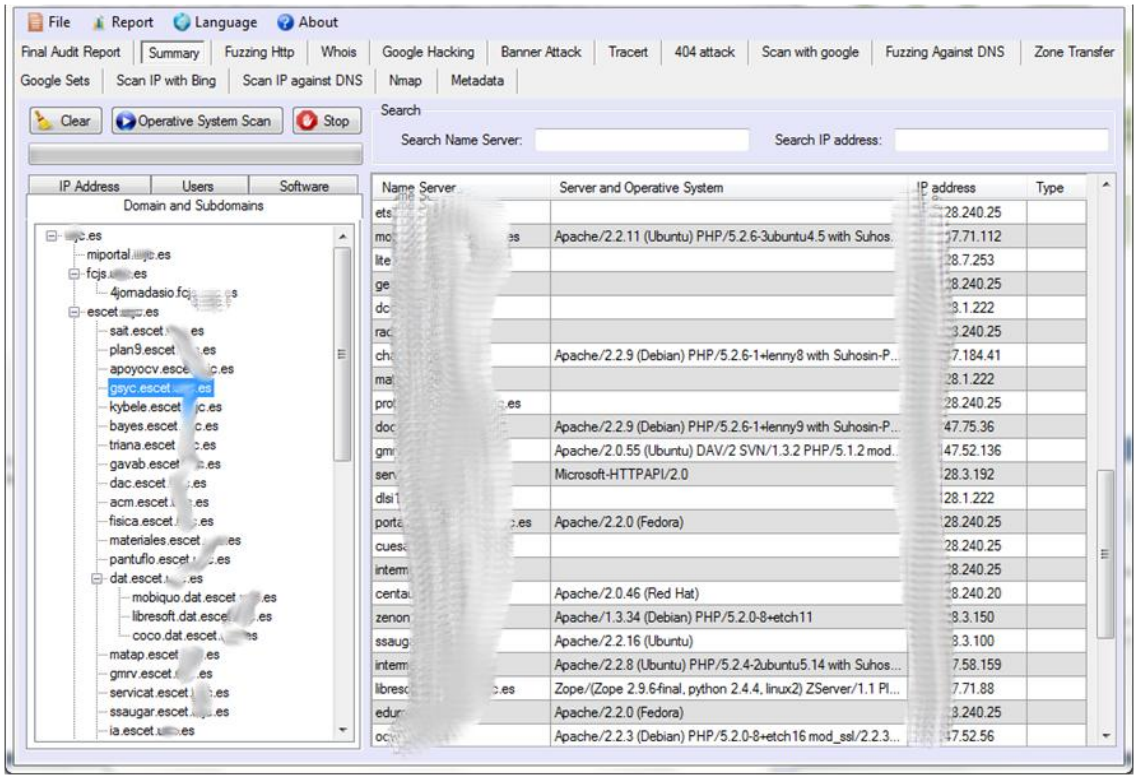
Para facilitar las cosas, en la herramienta Anubis, de la que ya hemos hablado, hemos automatizado esta operación, por lo que para visualizar el banner nos bastará con colocar el dominio y pulsar el botón Blind Scan:




Para automatizar más aún las cosas, una vez que hayáis encontrado varios subdominios/IPs, etc., por ejemplo por los métodos de búsqueda con buscadores que vimos en el primer artículo de la cadena (pestaña Scan with Google de Anubis), si pulsamos el botón “send”, nos almacenará toda esta información en una tabla resumen que podéis ver en la pestaña “summary”:

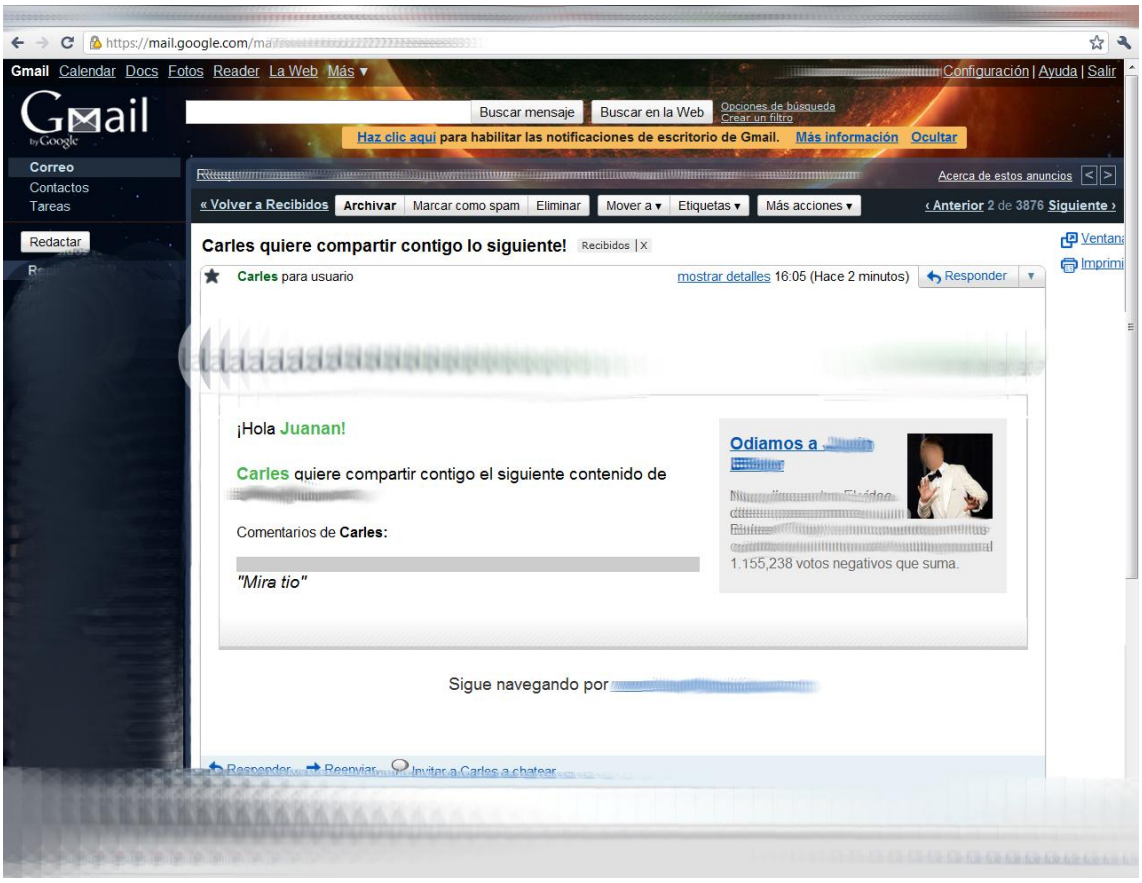


Si ahora pulsamos sobre el botón “Operative System Scan”, Anubis intentará visualizar el sistema operativo y modelo del servidor Web mediante la consulta del banner de todas las máquinas que haya en la lista resumen actualmente:

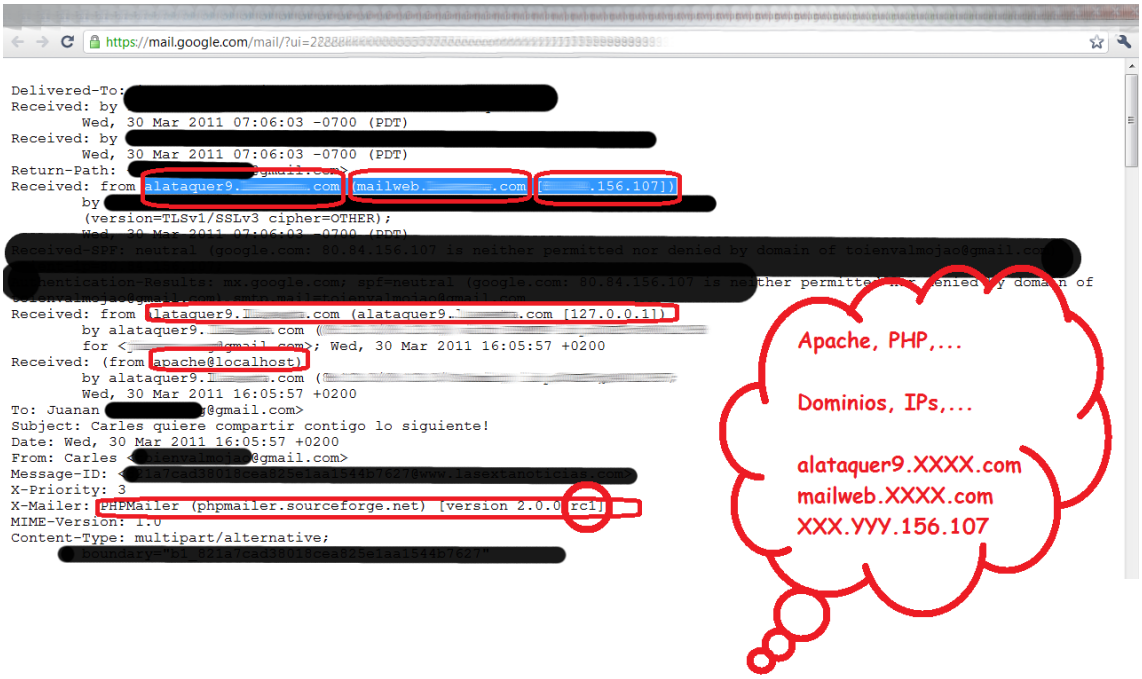



Como veis más sencillo no se puede tener. Otra manera de averiguar estos datos es la consulta de los servicios Web que utilizamos en el segundo artículo de la cadena.

Finalmente, la última técnica que veremos será el análisis de cabeceras de los correos electrónicos. Para ello, será clave que consigamos que alguien de la organización a auditar nos envíe un email, o tengan un sistema con el que podamos enviarlo nosotros mismos, como los típicos de “enviar esta noticia a un amigo”:




Y si analizamos el correo completo…:




Podemos utilizar otras herramientas, como por ejemplo Nmap, para intentar averiguar el sistema operativo de una máquina, pero sería Fingerprinting (activo)

ya que hay que forzar al servidor a que nos muestre la información, y eso se sale de la temática de este libro.

## 5. OBTENER INFORMACIÓN DE LOS DNS

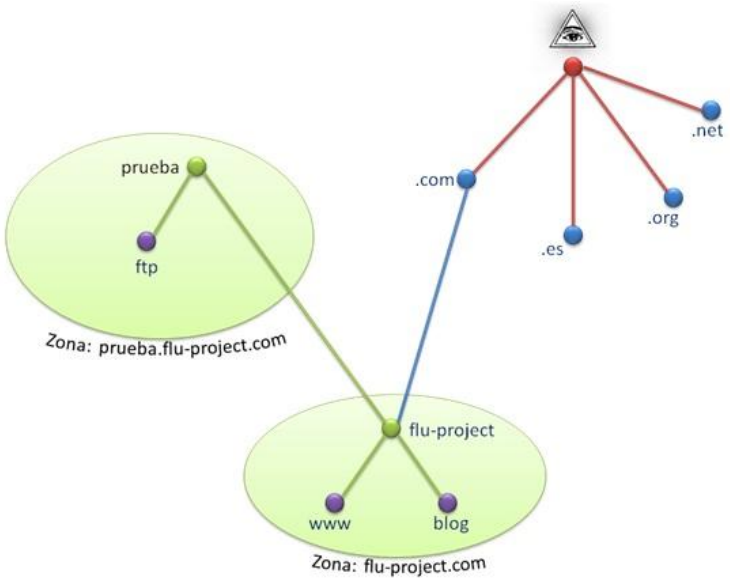
Para obtener información de los DNS vamos a utilizar cuatro técnicas diferentes:

- Forzar transferencias de zona
- Resolución inversa (a partir de una IP) mediante la consulta a los registros PTR
- Ataques de fuerza bruta mediante fuzzers o por diccionario
- Ataques de fuerza bruta mediante identificación de relaciones

Todos ellos los haremos a la vez con la herramienta Anubis y con la herramienta Nslookup, que tenéis disponible para Windows y Linux. Nosotros utilizaremos la versión para Windows, que cambian los comandos mínimamente con respecto a la versión de Linux.

- **Forzar transferencias de zona**

Para comenzar os hemos dibujado un diagrama muy ilustrativo sobre cómo funcionan las zonas, en él os mostramos nuestro dominio flu-project.com, con su nombre de dominio "flu-project" dentro de la zona principal. Por otro lado tenemos tres subdominios "blog", "www" y "ftp" (hipotéticos), estos subdominios pueden configurarse dentro de la zona principal, o en otra separada, como por ejemplo el caso del subdominio "ftp", que estaría administrado por la zona "prueba".



Para que una zona nueva delegada de la principal, por ejemplo la zona prueba, funcione, es necesario configurar algunos recursos, para que tenga información sobre la delegación a los otros servidores de DNS autorizados. Es de extrema importancia que las zonas estén disponibles desde varios servidores de DNS por temas de disponibilidad.

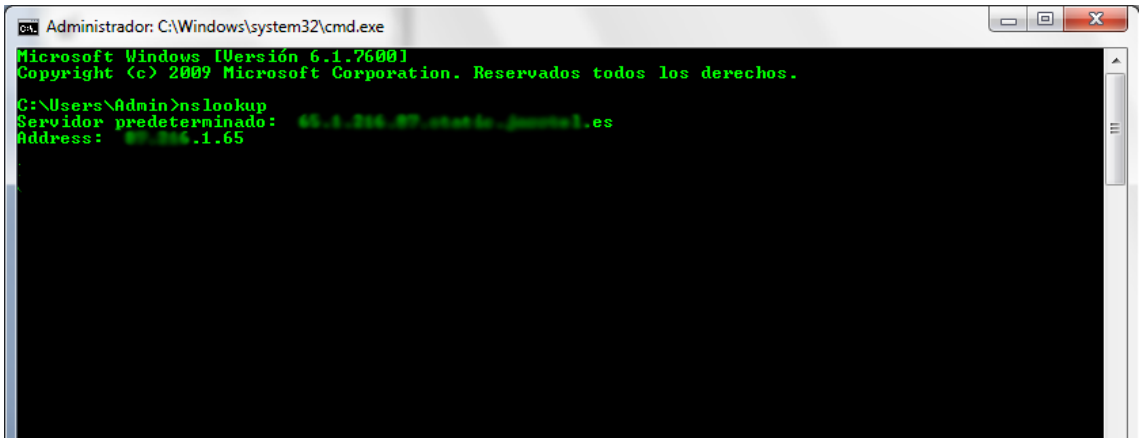
Para que otros servidores además del principal puedan alojar zonas, se crearon las transferencias de zona, que se encargan de hacer la replicación de todas ellas y de sincronizarlas.

Ahora bien, ¿cuándo se realizan estas transferencias de zona? Tenemos cuatro posibilidades:

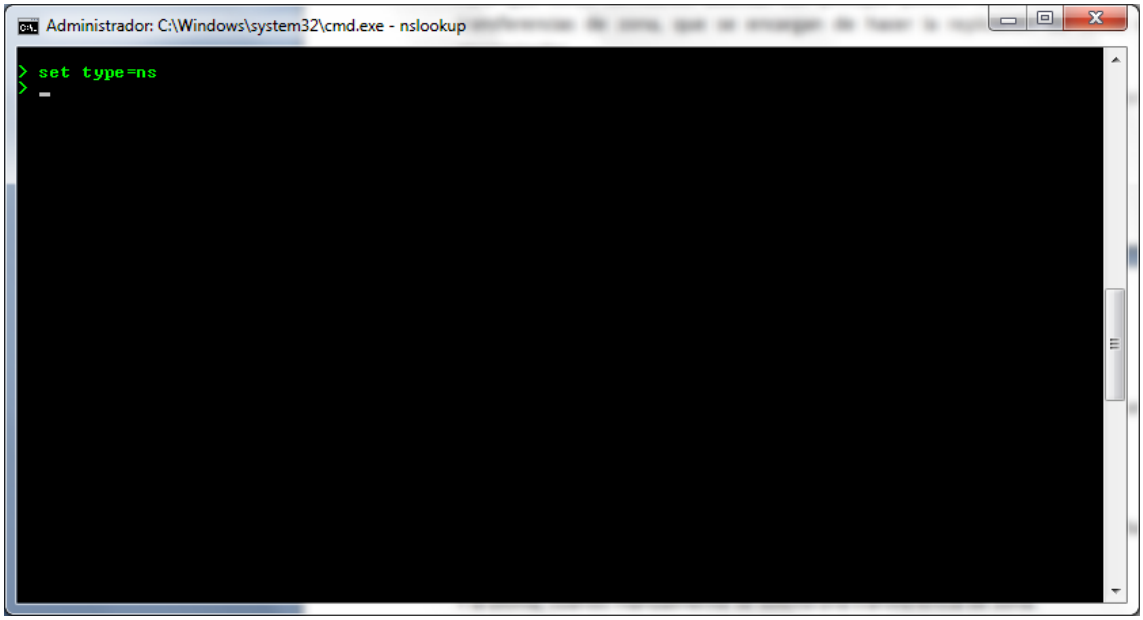
1. La primera de ellas es que se instale o inicie un nuevo servidor DNS y se configure en una zona existente.
2. La segunda, cuando finaliza el plazo de actualización de una zona.
3. La tercera, cuando se produce algún cambio en una zona, y es necesario actualizar para replicar los cambios.
4. Y la última, cuando manualmente se solicita una transferencia de zona.

Una vez entendido el concepto de zona, vamos a llevarlo a la práctica. Vamos a abrir una consola de comandos de Windows y ejecutaremos el programa “nslookup”. Nslookup es una aplicación de línea de comandos que permite probar y solucionar problemas en los servidores DNS. Nosotros lo utilizaremos para activar una transferencia de zona de manera manual.

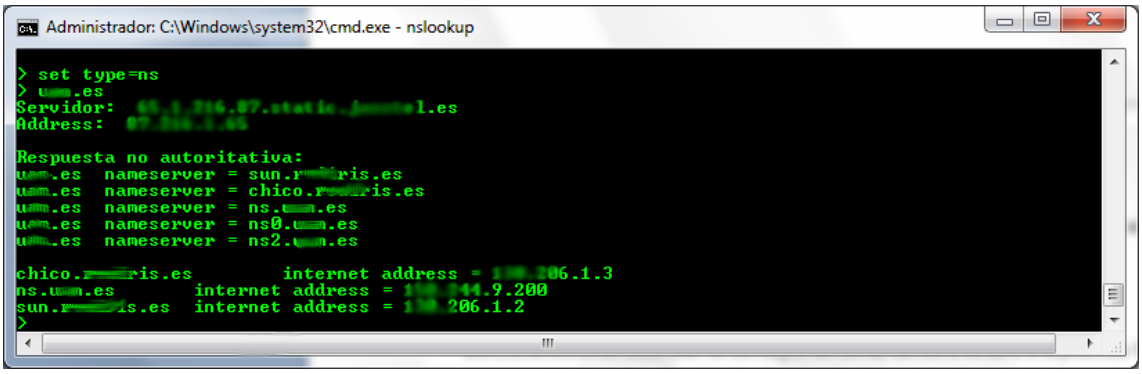
Vamos a iniciar Nslookup en modo interactivo, para ello basta con abrir un CMD y escribir el comando “nslookup”:




Ahora vamos utilizar la instrucción SET TYPE para consultar datos de tipo DNS (NS), para ver otros tipos de consultas podéis utilizar la ayuda poniendo una interrogación?:

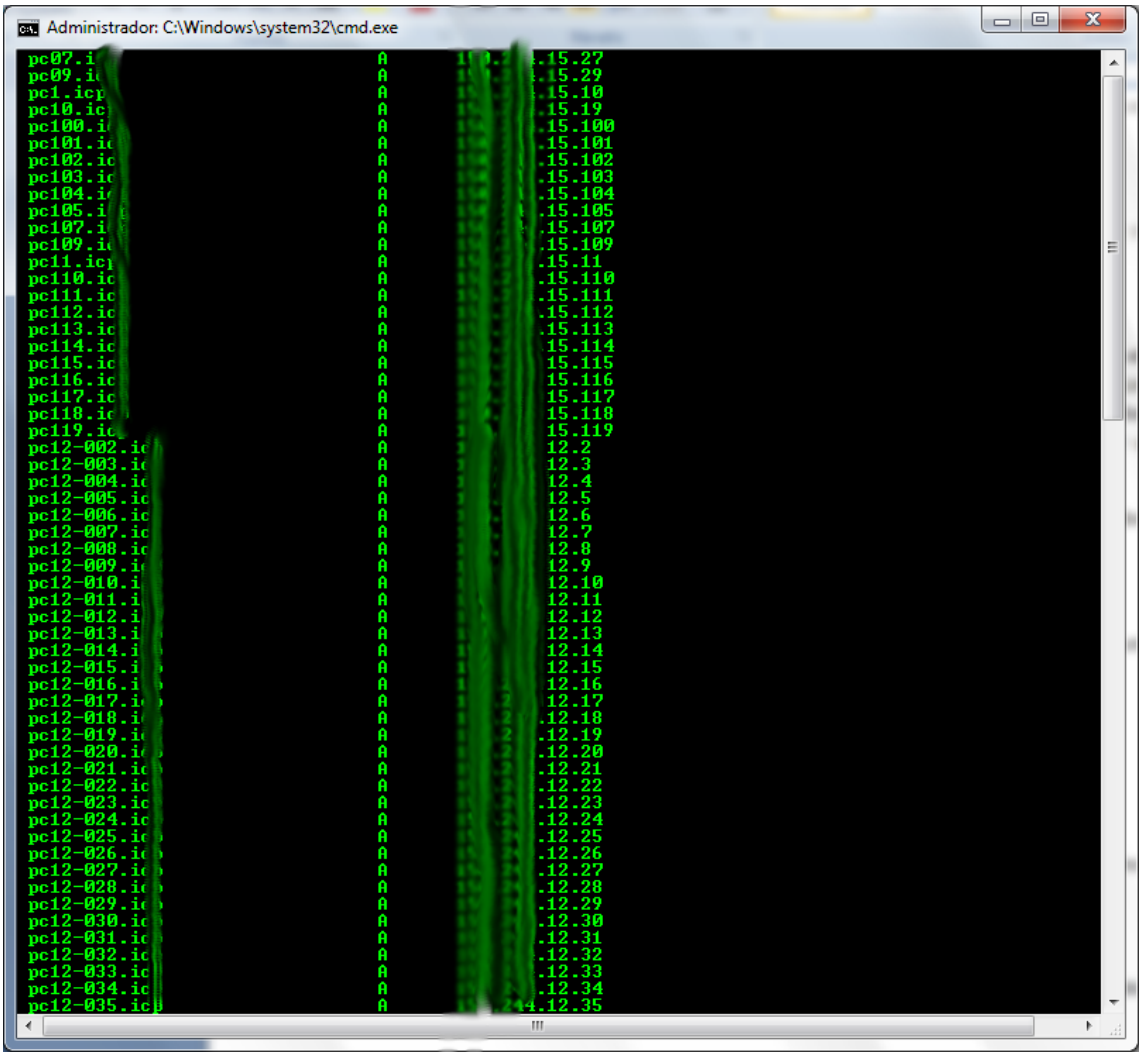



Ahora buscaremos los servidores de DNS de nuestro objetivo:



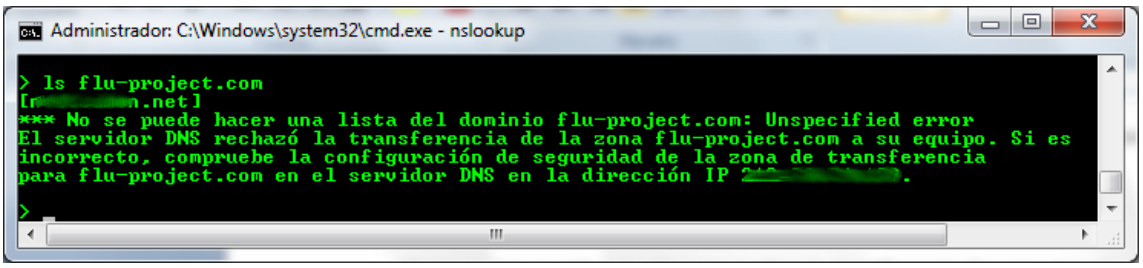

Ya sabemos los servidores DNS de ese dominio, ahora procederemos a ponernos como uno de ellos:


Ahora ya nos queda tan solo para realizar la transferencia de zona ejecutar el comando LS contra el dominio que queramos (ls dominio.com). Y disfrutar de todo el listado de máquinas que contienen las zonas:

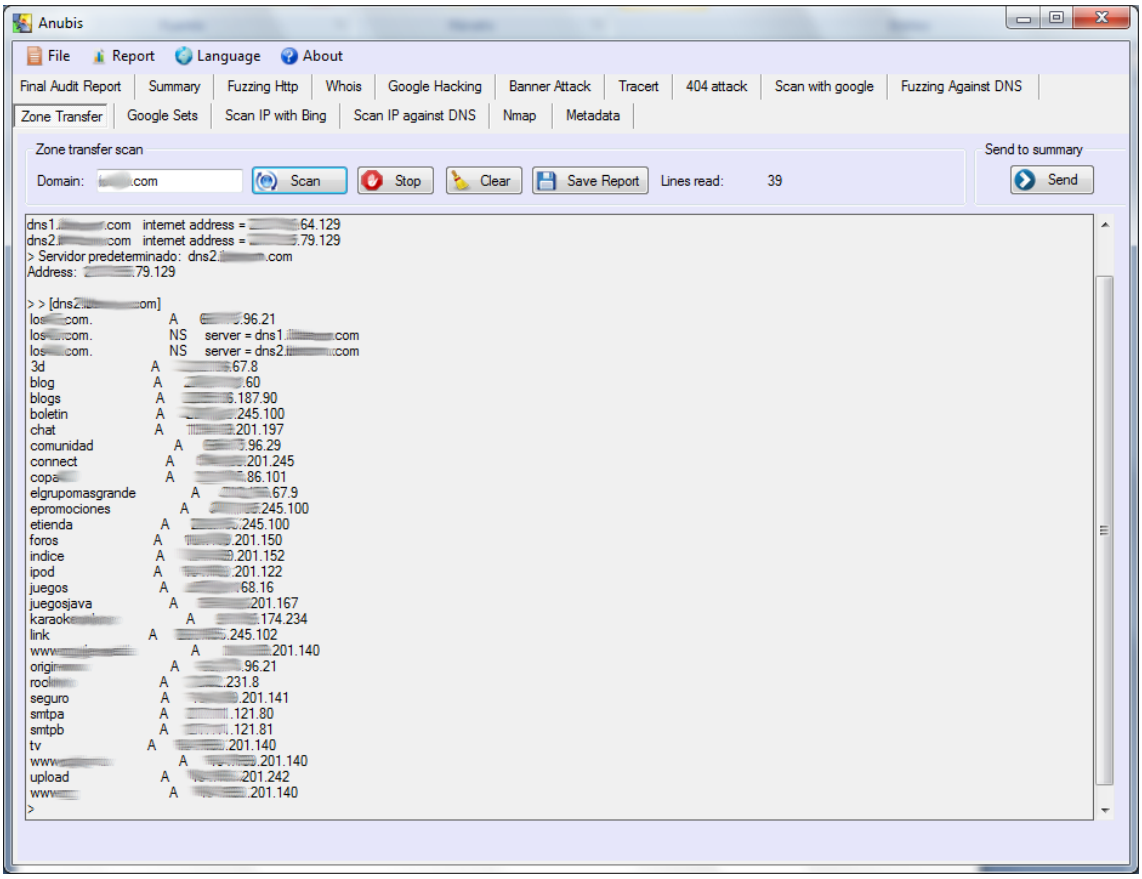



La transferencia de zona la hemos realizado desde fuera de la red interna debido a una mala configuración por parte de la organización. Esto no debería ocurrir, por motivos de seguridad obvios, y es que cualquiera desde su casa puede hacerse con todas las IP y dominios internos de una organización.

Para que estuviese bien configurado, nos debería haber respondido al comando LS con algo como lo siguiente:



Para facilitar la tarea, en Anubis se ha incorporado un módulo que es capaz de realizar una transferencia de zona con un solo clic:




- **<u>Resolución inversa (a partir de una IP) mediante la consulta a los registros PTR.</u>**

Lo más habitual es utilizar los DNS para obtener una IP, pero habrá ocasiones en la que nos interese lo contrario, dada una IP averiguar el DNS. A este hecho se le conoce como resolución inversa, y es utilizado normalmente para comprobar la identidad de un cliente.

Existe un dominio, el in-addr.arpa donde se encuentran las direcciones IP de todos los sistemas pero colocados de manera invertida, es decir, para la IP 193.X.Y.Z, le correspondería el nombre Z.Y.X.193.in-addr.arpa, y esto queda definido en los registros PTR, de donde intentaremos obtener la información.

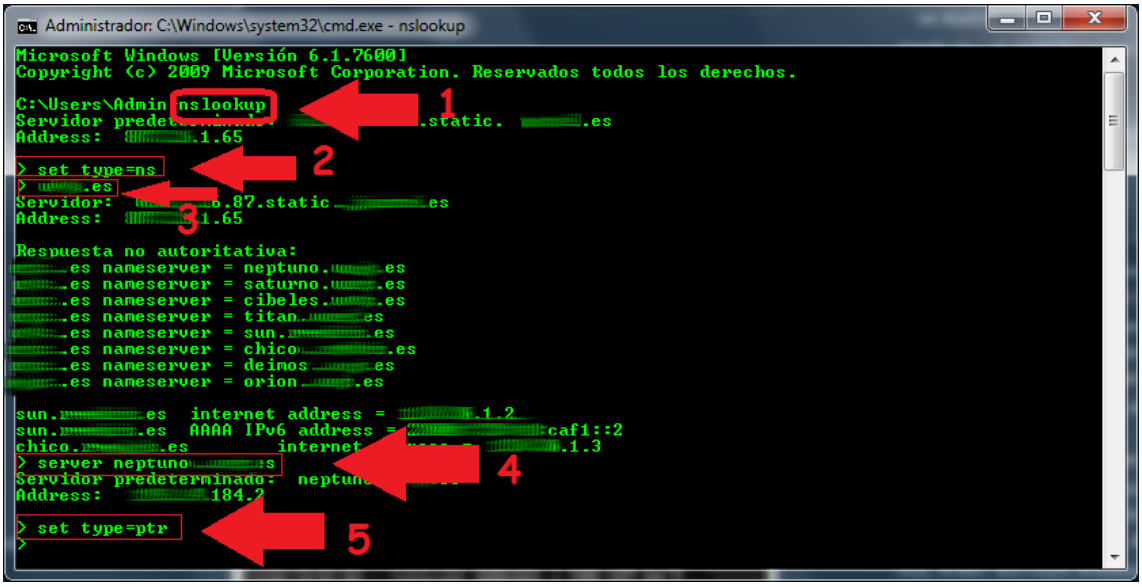
La idea es hacer lo siguiente, sabemos una dirección IP, que hemos encontrado mediante alguna de las búsquedas que aprendimos a realizar en los artículos 1 y 2 de esta cadena, pero no sabemos el nombre del dominio DNS, por tanto buscaríamos la query:

Z.Y.X.193.in-addr.arpa -> pericoeldelospalotes.com

Y verificaríamos que:

pericoeldelospalotes.com -> 193.X.Y.Z

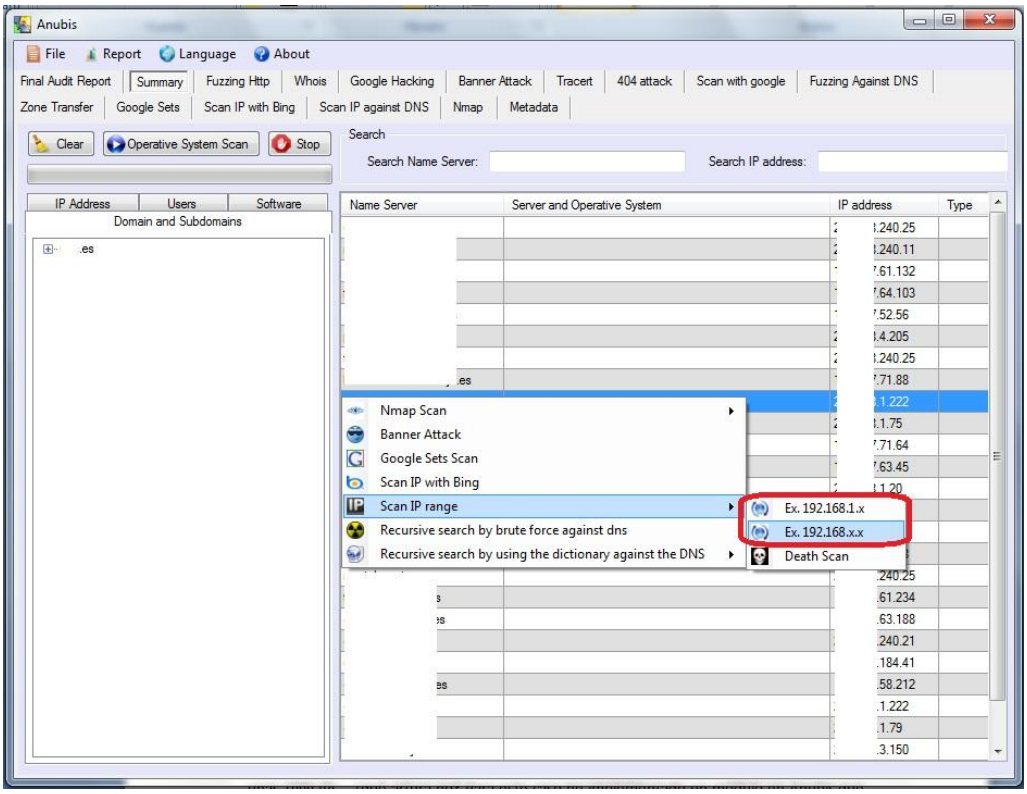
Para ello volveremos a utilizar la herramienta Nslookup. Configuraremos el DNS interno de la organización y configuramos el type para preguntar por los registros PTR:

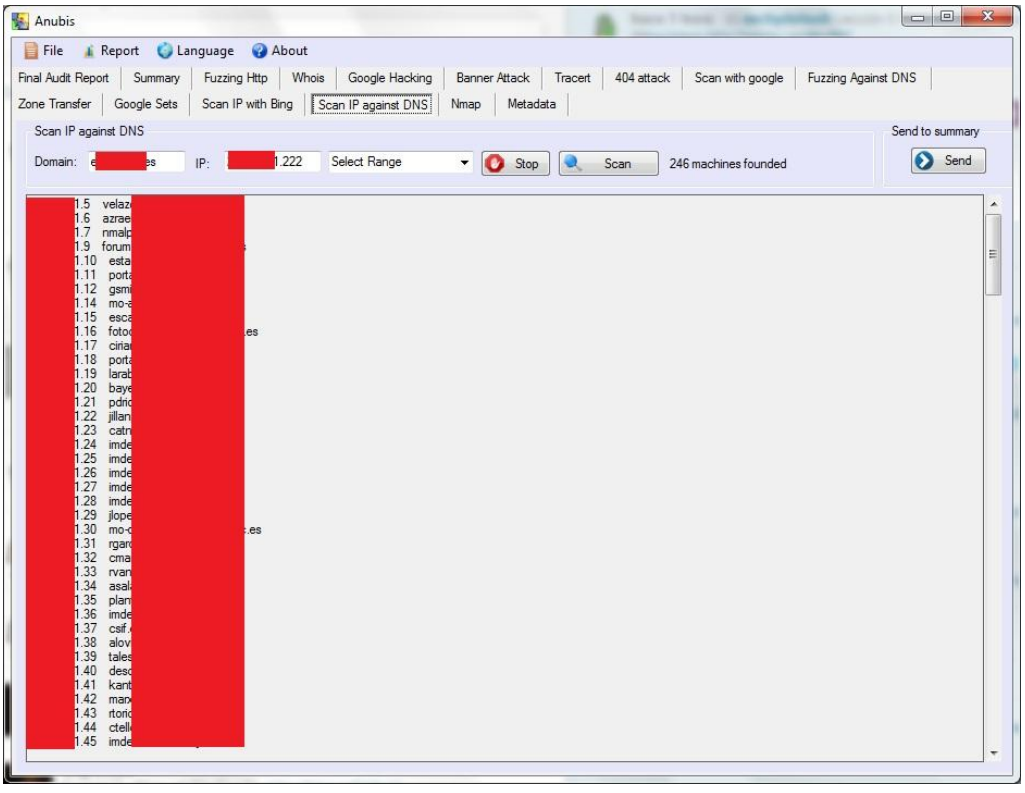



Y realizamos las búsquedas con algunas IP que habíamos encontrado:


Como veis una no se ha resuelto, por lo que no existe, pero la otra sí que ha tenido éxito. Imaginaros el caso de organizaciones grandes, en las que tengáis que

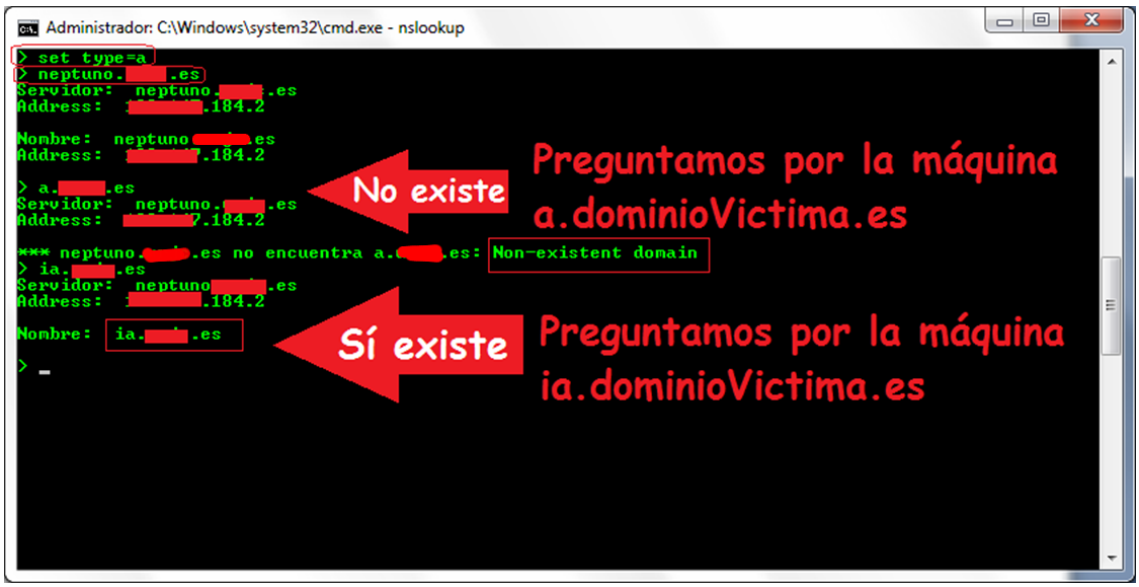
hacer éste proceso para unas 1000 IPs… ¿qué hartura no? Para éste caso hemos implementado un módulo en Anubis que permite hacer la resolución inversa de DNS por rangos de IP de manera automatizada, simplemente habiendo encontrado previamente una dirección IP:



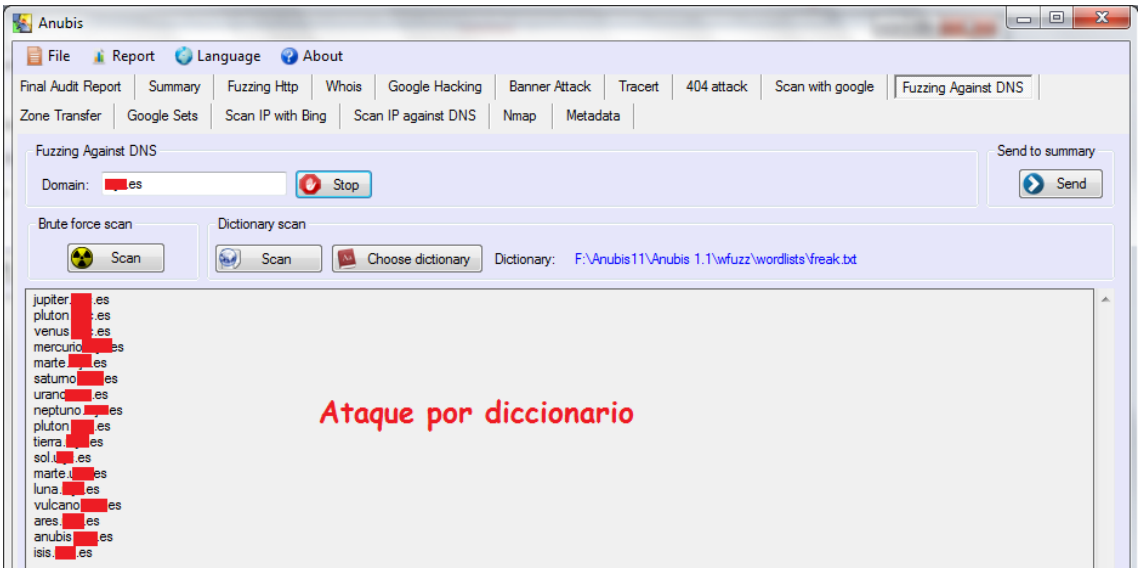
- **<u>Ataques de fuerza bruta mediante fuzzers o por diccionario.</u>**

Volveremos a configurar el DNS interno de la organización, pero ahora nos configuraremos en vez del tipo PTR el tipo A, con SET TYPE=A, para preguntar directamente por la existencia de máquinas. No sabemos el nombre de ninguna máquina, por lo que buscamos por ejemplo los subdominios a.dominioVictima.es e ia.dominioVictima.es:




Como veis, una de ellas sí existe.

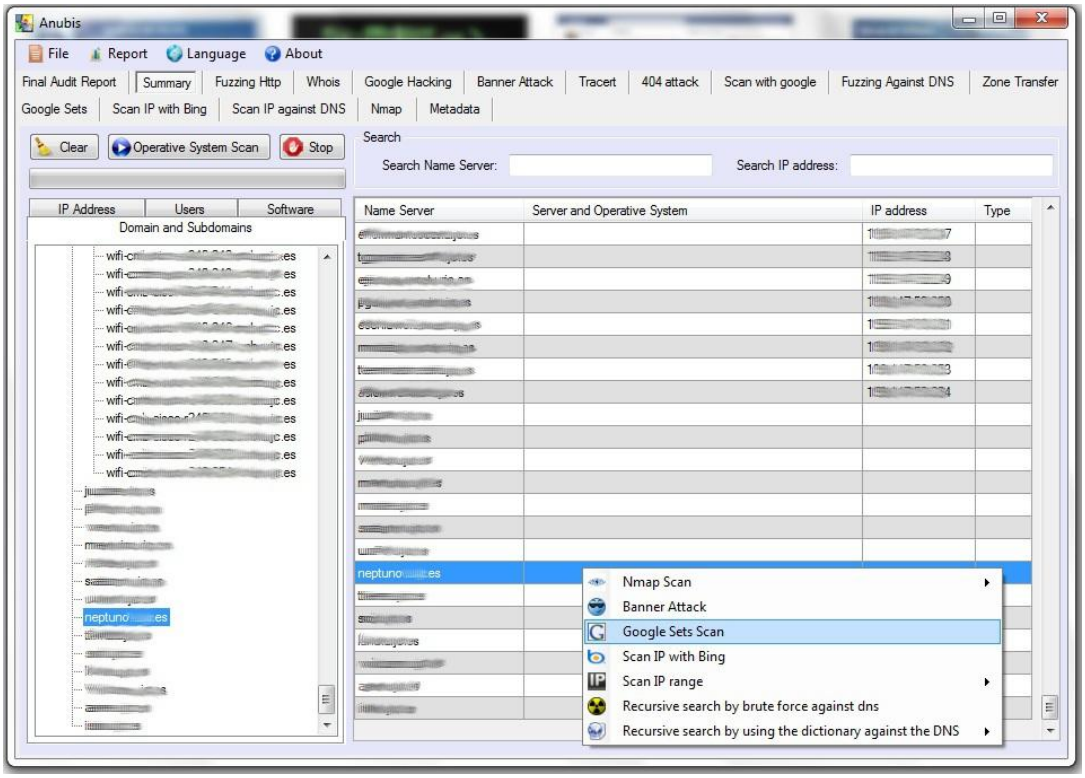
Anubis lleva incorporado un módulo de fuerza bruta que nos permitirá hacer fuerza bruta de esta manera contra el DNS, bien preguntando por palabras que irá generando mediante permutaciones de símbolos, letras y números, o bien preguntando por las palabras contenidas en un diccionario:



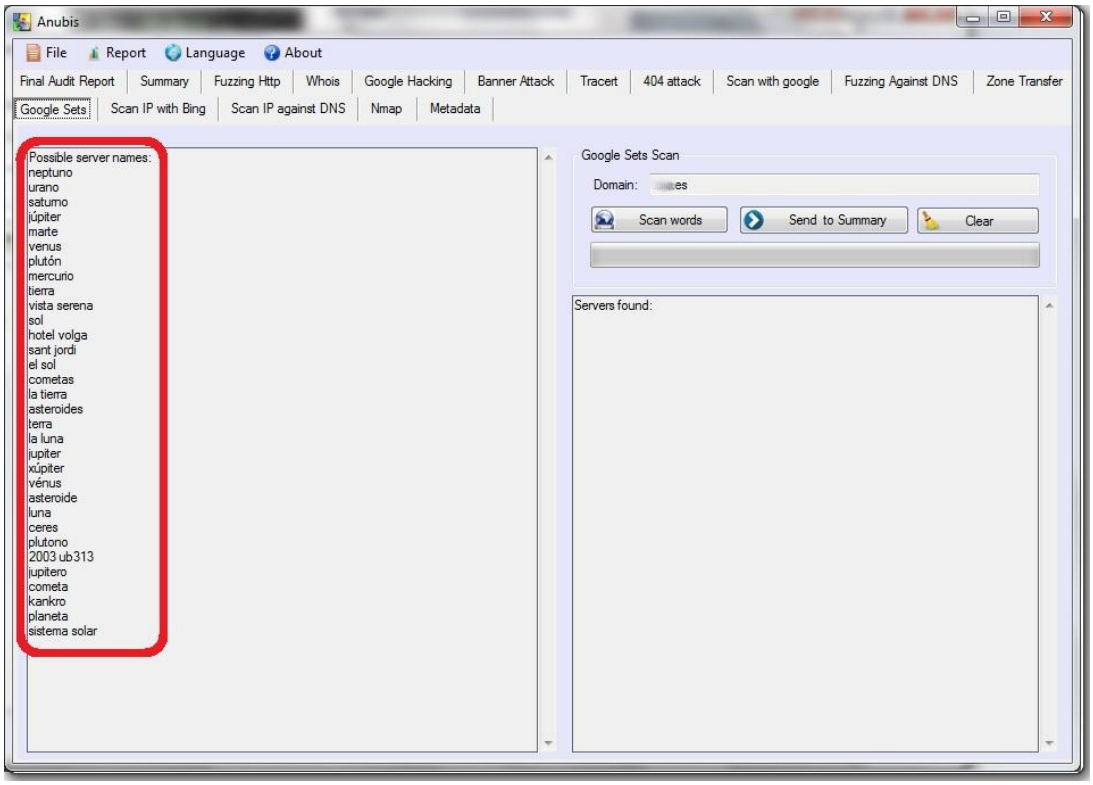

- **<u>Ataques de fuerza bruta mediante identificación de relaciones</u>**

Como habéis visto, con el ataque anterior hemos obtenido algunas máquinas con nombres curiosos y relacionados entre sí, como por ejemplo nombres de planetas y dioses.

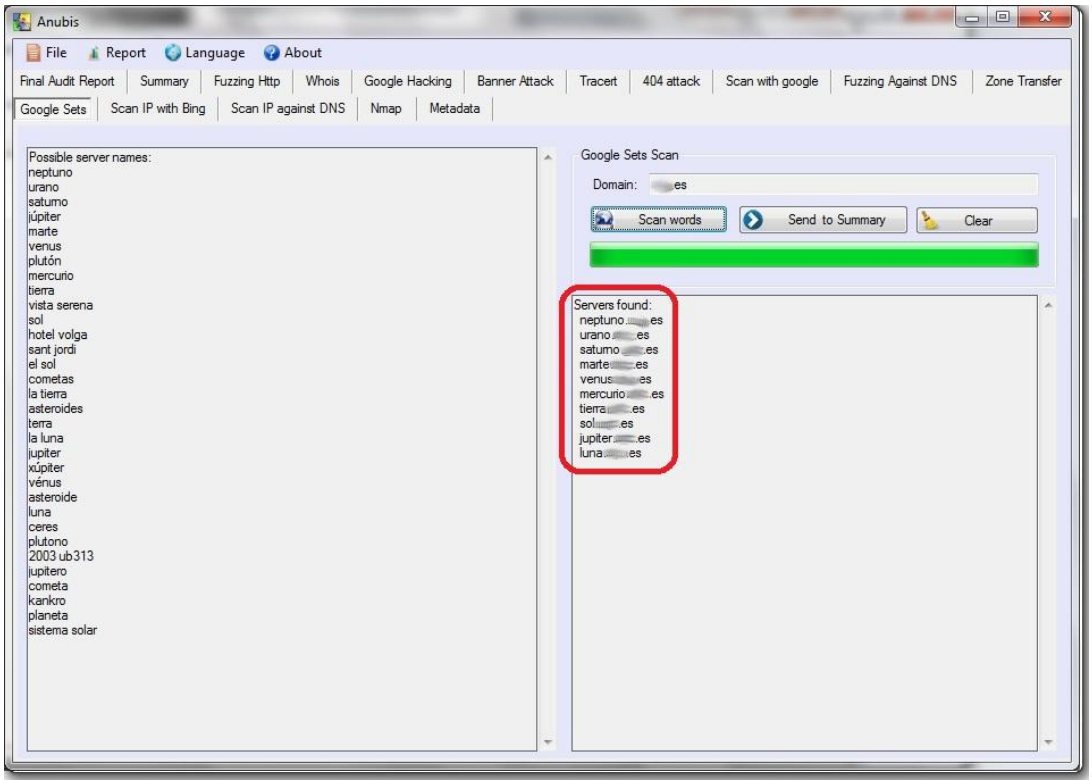
Ahora vamos a seleccionar por ejemplo neptuno, y vamos a utilizar la funcionalidad Google Sets, que nos permite encontrar listados de palabras relacionadas con una determinada palabra (por ejemplo si buscamos por Homer, nos devolverá resultados como Bart, Lisa, Magie, Nelson, Moe, etc.):



Como vemos, Google Sets ha encontrado varios términos relacionados con la palabra “neptuno”:




Ahora comprobaremos si existen subdominios con esos nombres:



Y… premio, tenemos un listado de subdominios reales.

## 6. FUZZEANDO WEBS

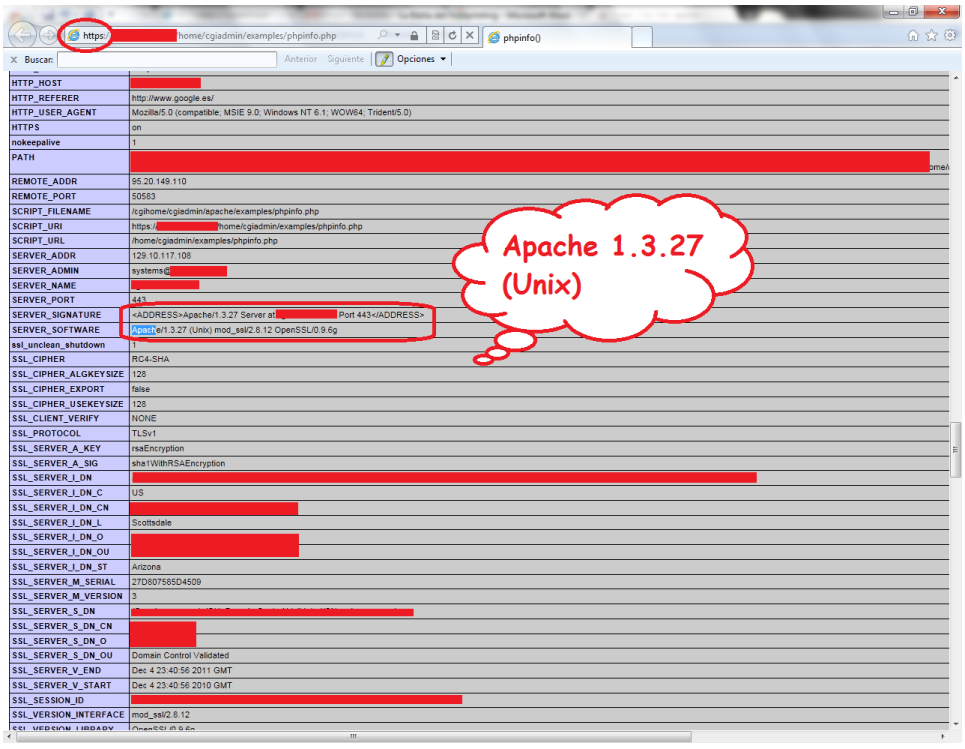
El siguiente paso será la búsqueda de páginas **no enlazadas** en un sitio web mediante ataques de fuerza bruta.

Por ejemplo, puede ocurrir que en la misma carpeta de una máquina donde se encuentra la página web (www, …) haya otro tipo de archivos que el webmaster utilice para sus quehaceres, pero que no tenga enlazados en el sitio Web, porque no es algo que los usuarios deberían ver. Por ejemplo, puede utilizar el servidor para compartir fotos suyas con un amigo, lo típico que las cuelga en un Zip, y les pasa el enlace directo a sus amigos para que las descarguen, o por poner otro ejemplo, un script de mantenimiento, o un panel de control, que no protege con contraseña porque piensa que si no está enlazado al sitio web nadie lo encontrará, o los típicos phpinfo.php, paneles de contol de joomla (/administrator) de wordpress (/wp-admin), etc.

Por si no sabéis como es un fichero phpinfo.php, una búsqueda en Google que os puede ayudar para ver alguno sería:

```
inurl:phpinfo.php ext:php -site:php.net
```

Son bastante interesantes ya que dan mucha información del servidor Web:



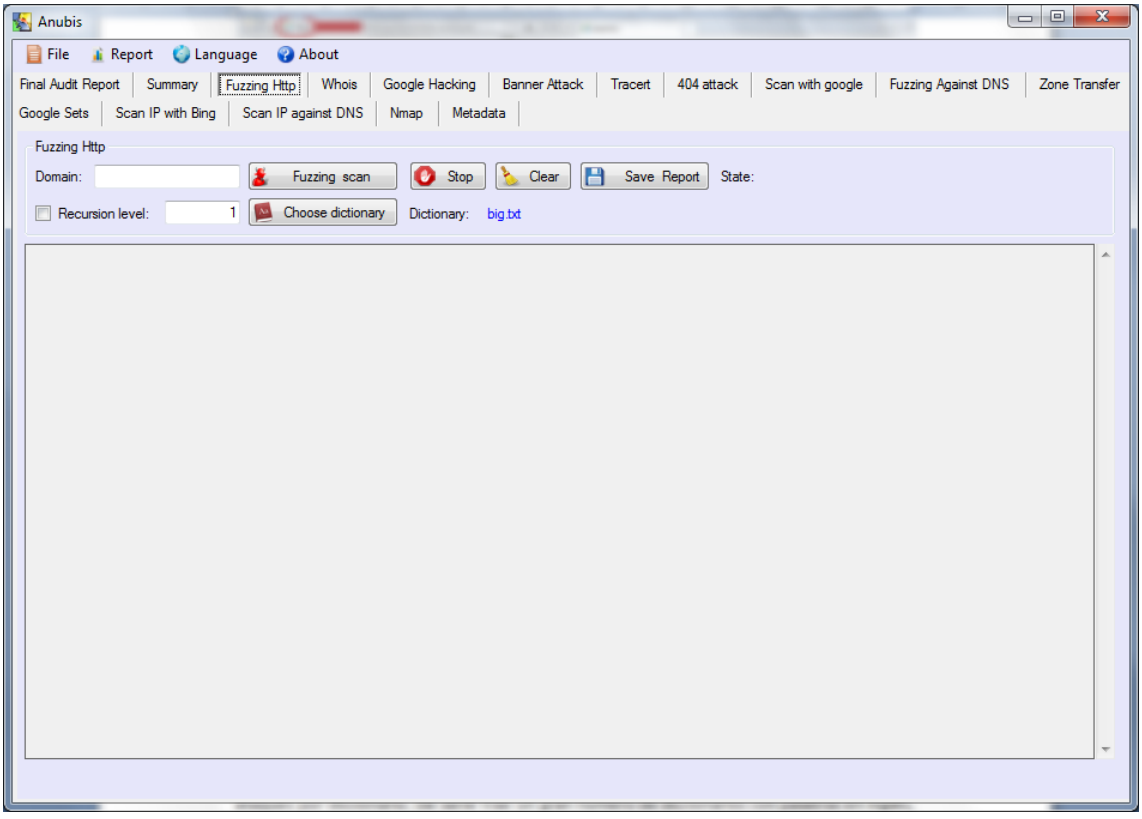
Otro fichero interesante que podemos buscar es el phpmyadmin. Para buscarlo por Google podéis utilizar la siguiente búsqueda-truco:

```
inurl:phpMyAdmin/Documentation ext:html
```

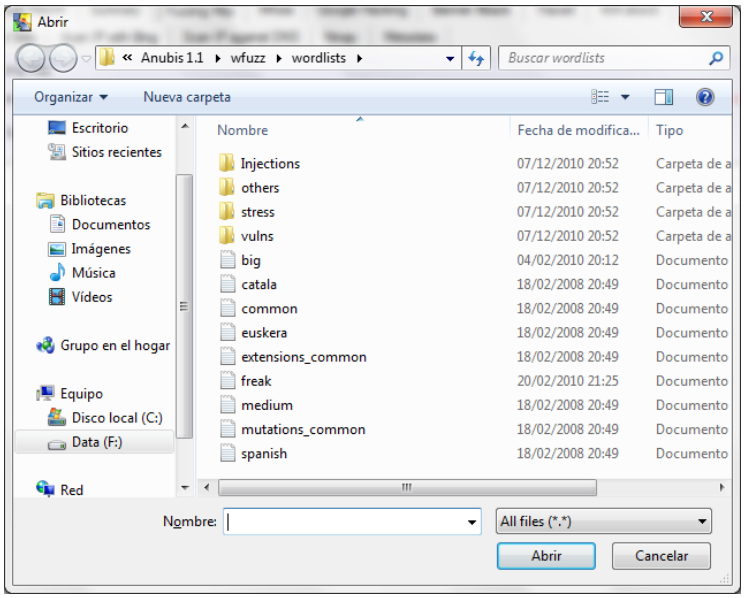
Y una vez que hayáis encontrado alguna página, quitáis de la URL la parte "/Documentation.html" y deberíais acceder al panel phpMyAdmin.

Ahora que ya sabemos qué tipo de ficheros nos interesaría encontrar, vamos a fuzzear. A nosotros el fuzzer que más nos gusta es Wfuzz. Es un programa de consola, fácil de integrar por tanto con otras aplicaciones, muy sencillo de utilizar y que nos permitirá hacer ataques por diccionario. De serie trae un gran número de diccionarios con palabras, posibles ficheros, inyecciones, etc. Anubis lleva una automatización de este fuzzer, al que hemos añadido de hecho un nuevo diccionario que se echaba en falta con palabras "freaks".

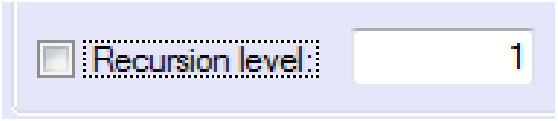
Para acceder a Wfuzz desde Anubis, debéis ir a la pestaña "Fuzzing http":



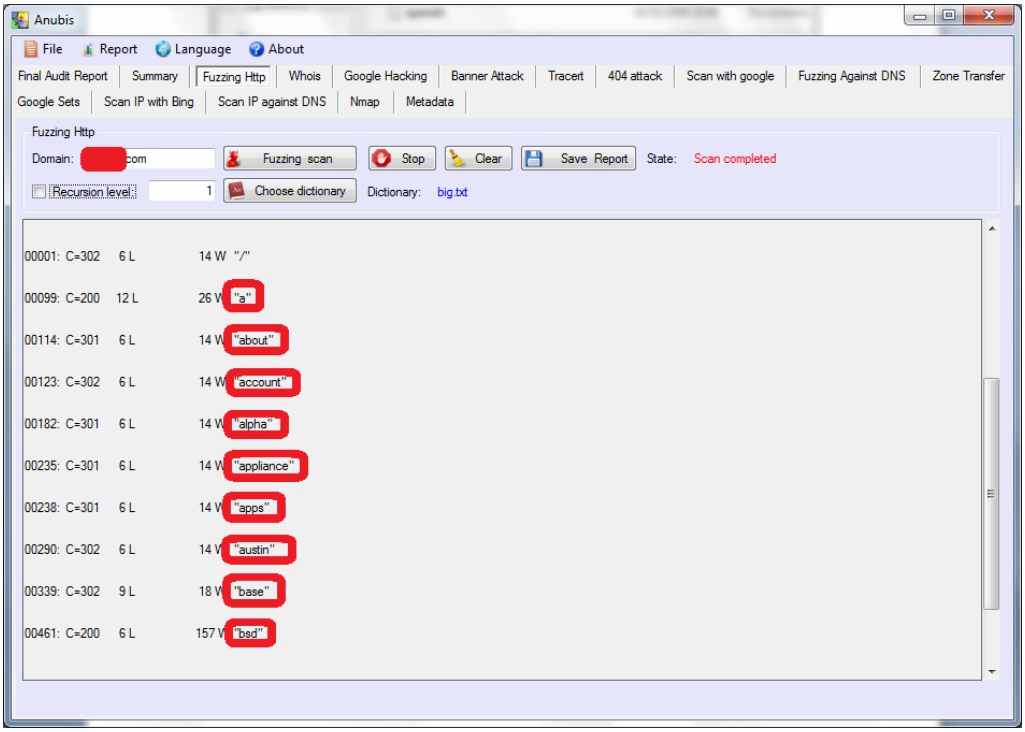

Pulsaremos en "Choose dictionary" para escoger un diccionario. Por ejemplo si vais a auditar un dominio .cat, pues puede ser interesante realizar un fuzzing con el diccionario "catala":




Ahora marcaremos Recursion level, si queremos que cada vez que encuentre una nueva ruta, vuelva a realizar un escaneo entero sobre ella. Podremos marcarle el número de recursiones que queremos realizar. Pero tened en cuenta que a más recursiones, más tiempo tardará en finalizar:




Y pulsáis el botón “Fuzzing scan”:



Como veis han aparecido algunos ficheros que empiezan por “a” y por “b” ya que hemos realizado un escaneo con el diccionario big.

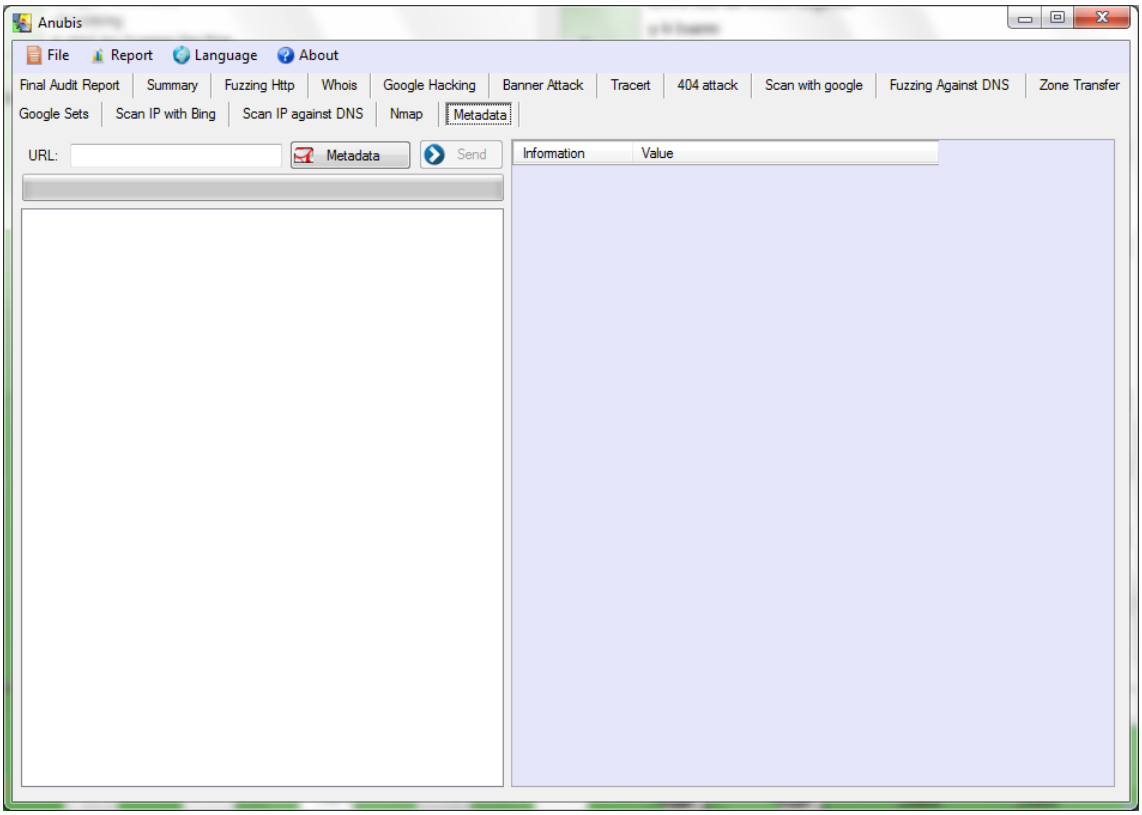
## 7. METADATOS

Como sabréis, los metadatos son una serie de datos que son almacenados junto con los documentos para ayudar en su identificación. Su intención es representar el contenido del documento, por lo que suelen almacenar bastantes datos, en ocasiones más de la que nos gustaría, lo que conlleva a que sea más fácil, por ejemplo, identificar al usuario que ha creado cierto documento, las herramientas con las que lo ha hecho, la situación física donde se encontraba, un path que puede darnos información del sistema operativo, etc. Este hecho trae repercusiones que pueden llegar a ser muy graves, pongamos por ejemplo que a través de un metadato se averigua que se ha generado un documento con una versión de cierto programa para generar ficheros PDF que tiene un exploit conocido; entonces se estaría poniendo en peligro un sistema. Otro ejemplo que ha traído una gran repercusión hace unos meses fue el de la caza de unos pederastas a través de la información de los metadatos del posicionamiento por GPS de las fotos realizadas con un iPhone y que compartían por foros de Internet. Por lo que parece que los metadatos pueden ser más peligrosos de lo que inicialmente parece.

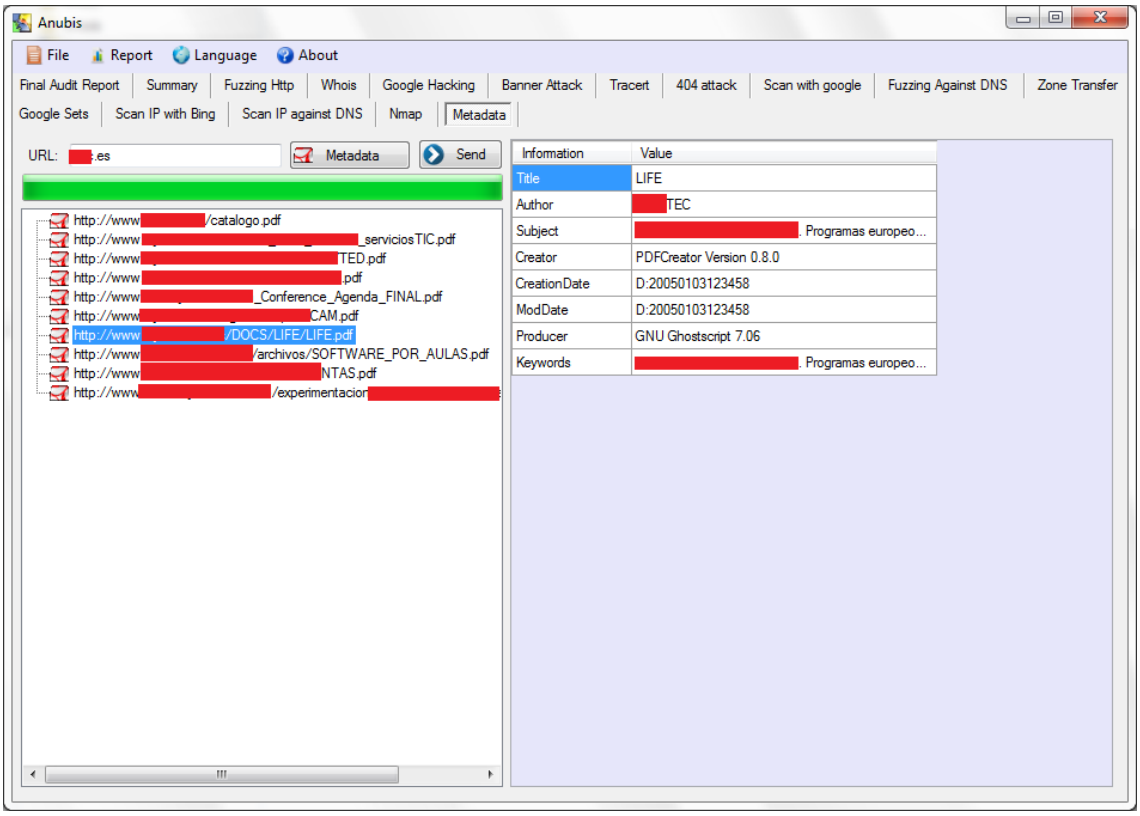
Para extraer los metadatos de los documentos y hacerles un footprinting, existen multitud de servicios online y herramientas que automatizan esta tarea, pero hay una destaca por encima de todas, y esta es la FOCA. Podéis encontrar un interesante manual de esta herramienta en éste artículo.

Como no podía ser menos, nosotros también hemos querido hacer una pequeña aportación a la fase de Footprinting con Anubis, y añadímos en la versión 1.1 el primer módulo de análisis de metadatos, que es capaz de analizar los metadatos de los ficheros PDF y realizar listados de usuarios y de software encontrado, para ayudaros en la búsqueda de posibles exploits.

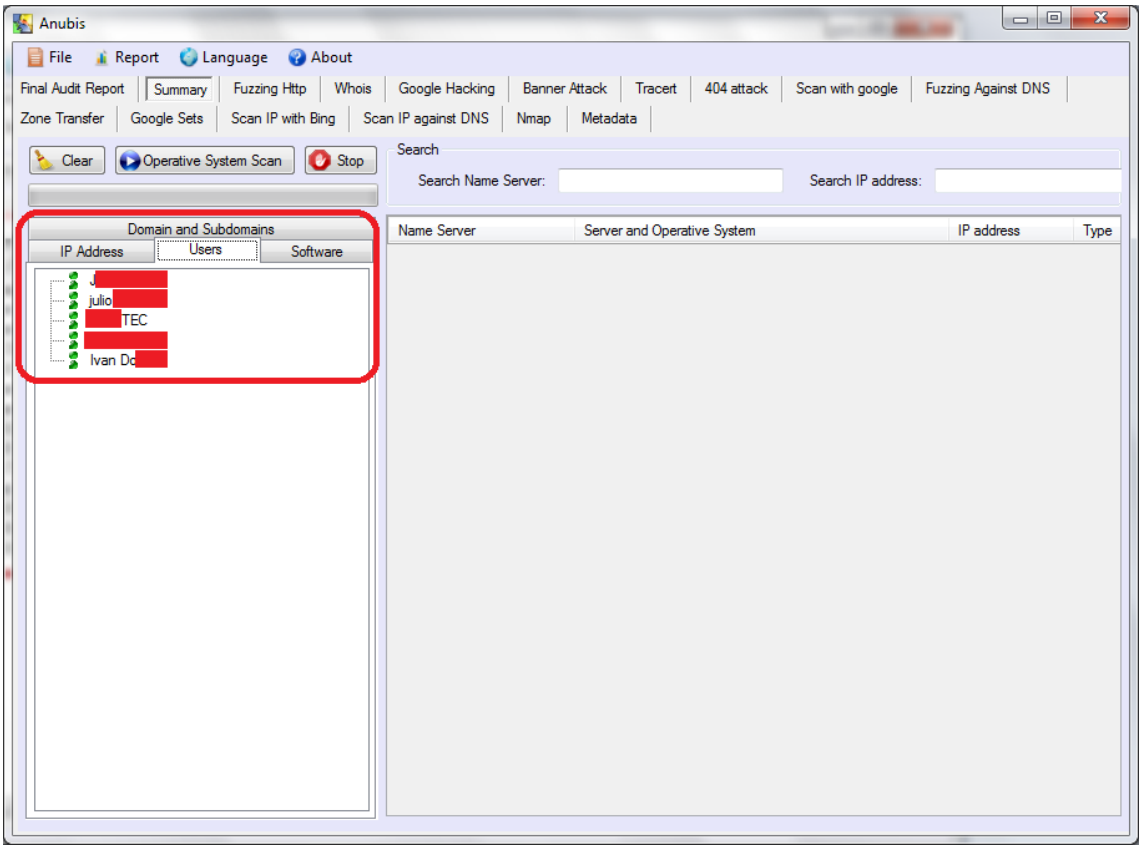
Si abrís Anubis y vais a la sección “Metadata” os encontraréis con la siguiente pantalla:

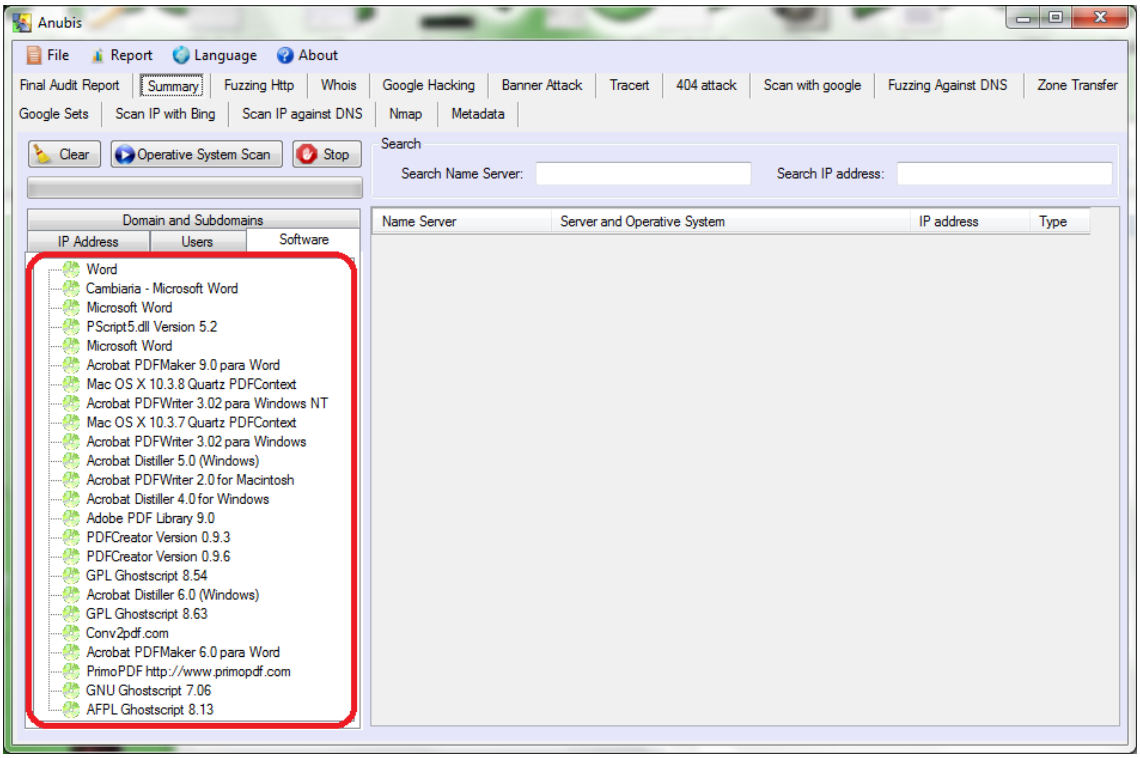



El funcionamiento es tan sencillo como poner un dominio y pulsar el botón "Metadata". Cuando la barra de progreso llegue al final ya podréis ver los metadatos de los ficheros PDF mostrados en el árbol de la ventana izquierda:



Ahora si pulsáis sobre el botón “SEND”, se enviará la información a la pestaña “SUMMARY”, donde se listarán todos los usuarios y software encontrados:



## REFLEXIONES FINALES

Con este libro habréis podido analizar algunas técnicas con las que realizar la búsqueda inicial de los datos necesarios para realizar un Test de Intrusión o una auditoría de Caja Negra.

El éxito del resto de las fases de la auditoría es directamente proporcional a la cantidad de información encontrada en la fase de footprinting, ya que será la que nos enseñará las puertas que en la fase de explotación intentaremos abrir.