



# **Extraer información pública de los dominios de Internet (espiando empresas)**

Alfredo Abad

UA: 13-ago-2018

PARP409-InforDominios.pptx

## **Objetivo**

- Conocer las herramientas de gestión de datos de registro para la arquitectura TCP/IP
- Estudio de las herramientas whois, nslookup, host
- Comprensión de la geolocalización pública de los nodos
- Conocer qué información puede gestionarse para imaginar situaciones de defensa contra espionaje

Parte primera:

## ESTUDIO GENERAL DE ALGUNAS UTILIDADES

### Herramienta whois (comenzamos instalando whois)

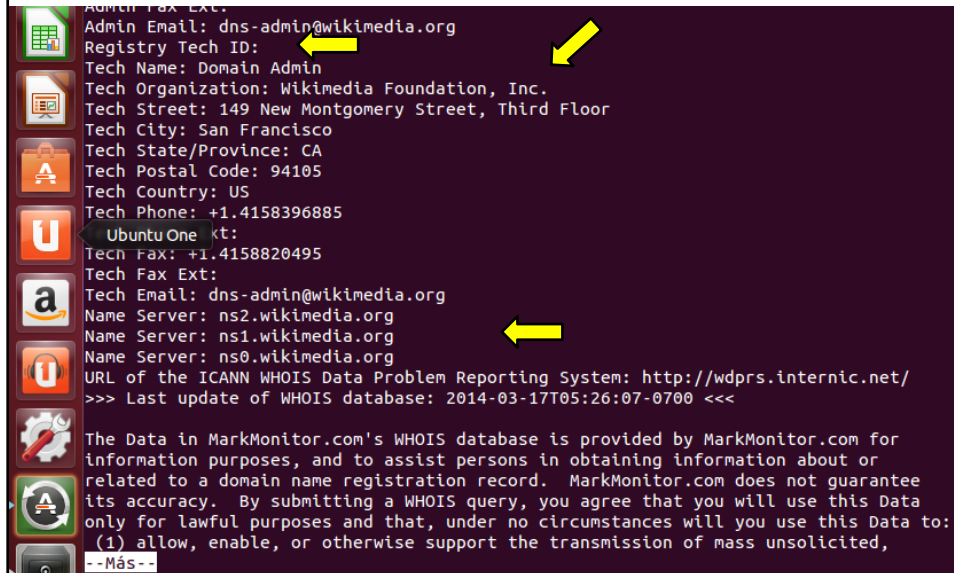
```
labadmin@ub32: ~  
labadmin@ub32:~$ sudo apt-get install whois  
Buscar en su equipo y en línea min:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  whois  
0 actualizados, 1 se instalarán, 0 para eliminar y 6 no actualizados.  
Necesito descargar 27,7 kB de archivos.  
Se utilizarán 139 kB de espacio de disco adicional después de esta operación.  
Des:1 http://es.archive.ubuntu.com/ubuntu/ raring/main whois i386 5.0.20ubuntu1 [27,7 kB]  
Descargados 27,7 kB en 3seg. (8.908 B/s)  
Seleccionando el paquete whois previamente no seleccionado.  
(Leyendo la base de datos ... 162672 ficheros o directorios instalados actualmente.)  
Desempaquetando whois (de .../whois_5.0.20ubuntu1_i386.deb) ...  
Procesando disparadores para man-db ...  
Configurando whois (5.0.20ubuntu1) ...  
labadmin@ub32:~$
```

## Ejecución de **whois wikipedia.com** (varias diapos)

```
labadmin@ub32: ~  
Whois Server Version 2.0  
Domain names in the .com and .net domains can now be registered  
through different competing registrars. Go to http://www.internic.net  
for more information.  
  
Domain Name: WIKIPEDIA.COM  
Registrar: MARKMONITOR INC.  
Whois Server: whois.markmonitor.com  
Referral URL: http://www.markmonitor.com  
Name Server: NS0.WIKIMEDIA.ORG  
Name Server: NS1.WIKIMEDIA.ORG  
Name Server: NS2.WIKIMEDIA.ORG  
Status: clientDeleteProhibited  
Status: clientTransferProhibited  
Status: clientUpdateProhibited  
Updated Date: 09-mar-2012  
Creation Date: 12-jan-2001  
Expiration Date: 10-jan-2017  
  
>>> Last update of whois database: Mon, 17 Mar 2014 12:26:29 UTC <<<  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and  
Registrars.  
Domain Name: wikipedia.com  
Registry Domain ID: 51687032_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2013-09-13T04:00:11-0700  
Creation Date: 2012-02-10T09:16:09-0800  
Registrar Registration Expiration Date: 2017-01-09T21:28:20-0800  
Registrar: MarkMonitor, Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: compliance@markmonitor.com  
Registrar Abuse Contact Phone: +1.2083895740  
Domain Status: clientUpdateProhibited  
Domain Status: clientTransferProhibited  
Domain Status: clientDeleteProhibited  
Registry Registrant ID:  
Registrant Name: Domain Admin  
Registrant Organization: Wikimedia Foundation, Inc.  
Registrant Street: 149 New Montgomery Street, Third Floor  
Registrant City: San Francisco  
Registrant State/Province: CA  
Registrant Postal Code: 94105  
Registrant Country: US  
Registrant Phone: +1.4158396885  
Registrant Phone Ext:  
Registrant Fax: +1.4158820495  
--Más--
```

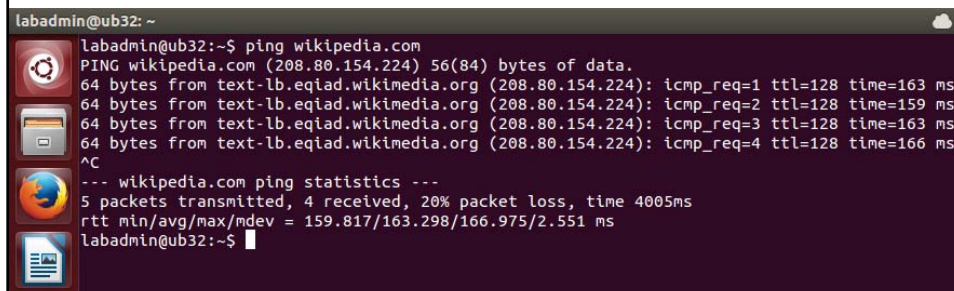
## Administrador técnico y DNS



```
Admin Fax Ext:
Admin Email: dns-admin@wikimedia.org
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Wikimedia Foundation, Inc.
Tech Street: 149 New Montgomery Street, Third Floor
Tech City: San Francisco
Tech State/Province: CA
Tech Postal Code: 94105
Tech Country: US
Tech Phone: +1.4158396885
UbuntuOne kt:
Tech Fax: +1.4158820495
Tech Fax Ext:
Tech Email: dns-admin@wikimedia.org
Name Server: ns2.wikimedia.org
Name Server: ns1.wikimedia.org
Name Server: ns0.wikimedia.org
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2014-03-17T05:26:07-0700 <<<

The Data in MarkMonitor.com's WHOIS database is provided by MarkMonitor.com for
information purposes, and to assist persons in obtaining information about or
related to a domain name registration record. MarkMonitor.com does not guarantee
its accuracy. By submitting a WHOIS query, you agree that you will use this Data
only for lawful purposes and that, under no circumstances will you use this Data to:
(1) allow, enable, or otherwise support the transmission of mass unsolicited,
--Más--
```

## Conseguir una IP del dominio (se puede hacer utilizando la resolución que disparará ping)



```
labadmin@ub32: ~
labadmin@ub32:~$ ping wikipedia.com
PING wikipedia.com (208.80.154.224) 56(84) bytes of data:
64 bytes from text-lb.eqiad.wikimedia.org (208.80.154.224): icmp_req=1 ttl=128 time=163 ms
64 bytes from text-lb.eqiad.wikimedia.org (208.80.154.224): icmp_req=2 ttl=128 time=159 ms
64 bytes from text-lb.eqiad.wikimedia.org (208.80.154.224): icmp_req=3 ttl=128 time=163 ms
64 bytes from text-lb.eqiad.wikimedia.org (208.80.154.224): icmp_req=4 ttl=128 time=166 ms
^C
--- wikipedia.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4005ms
rtt min/avg/max/mdev = 159.817/163.298/166.975/2.551 ms
labadmin@ub32:~$
```

## Utilidad dig

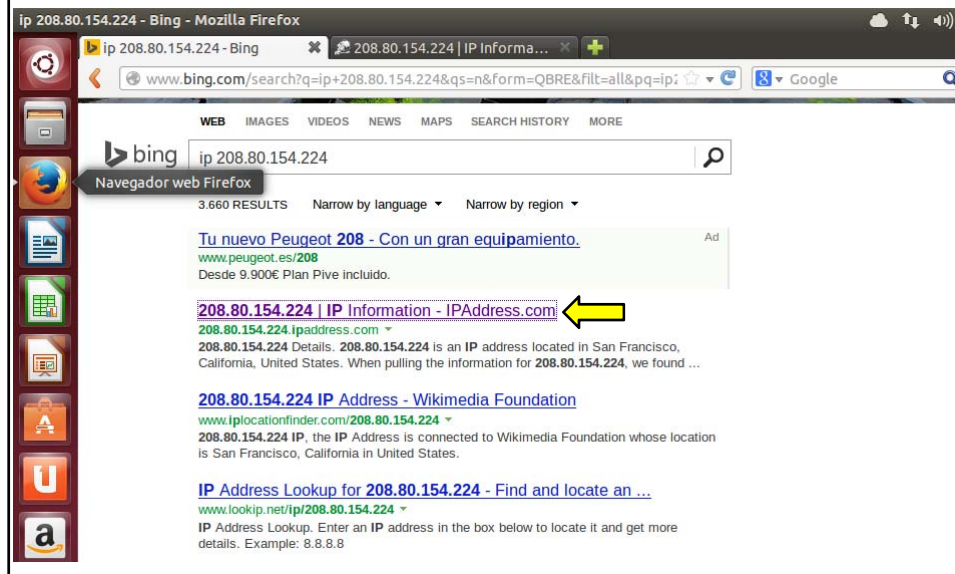
```
labadmin@ub32: ~  
labadmin@ub32:~$ dig www.wikipedia.com  
; <<>> DiG 9.9.2-P1 <<>> www.wikipedia.com  
;; gl  
;; Go LibreOffice Impress  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29531  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4000  
;; QUESTION SECTION:  
;www.wikipedia.com. IN A  
;; ANSWER SECTION:  
www.wikipedia.com. 5 IN CNAME wikipedia-lb.wikimedia.org.  
wikipedia-lb.wikimedia.org. 5 IN CNAME text-lb.esams.wikimedia.org.  
text-lb.esams.wikimedia.org. 5 IN A 91.198.174.192  
;; Query time: 3 msec  
;; SERVER: 127.0.1.1#53(127.0.1.1)  
;; WHEN: Mon Mar 17 14:03:22 2014  
;; MSG SIZE rcvd: 130  
labadmin@ub32:~$
```

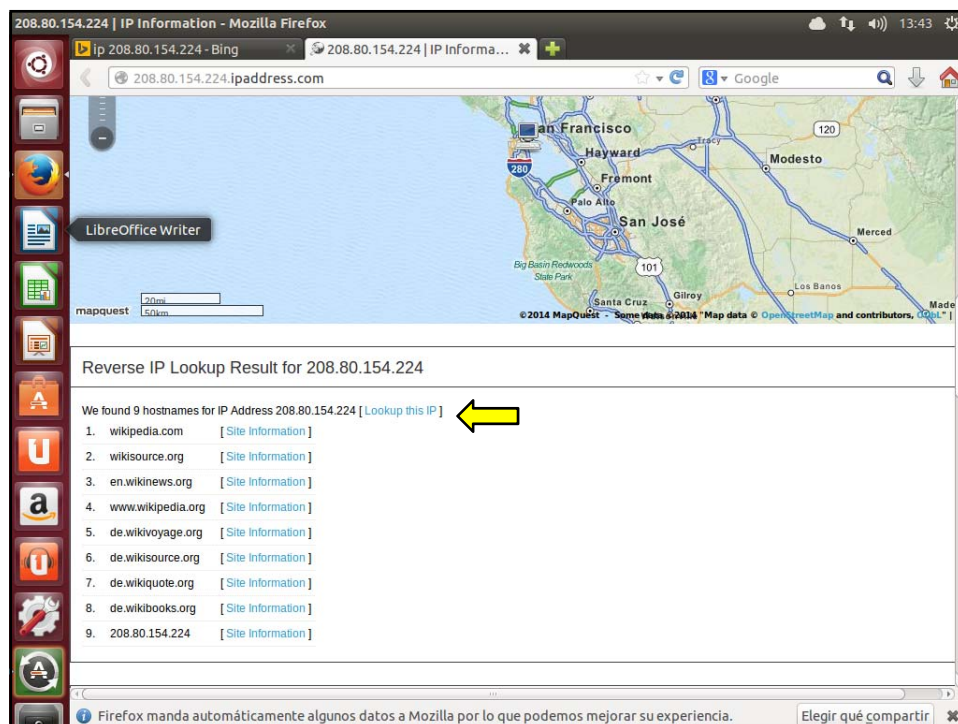
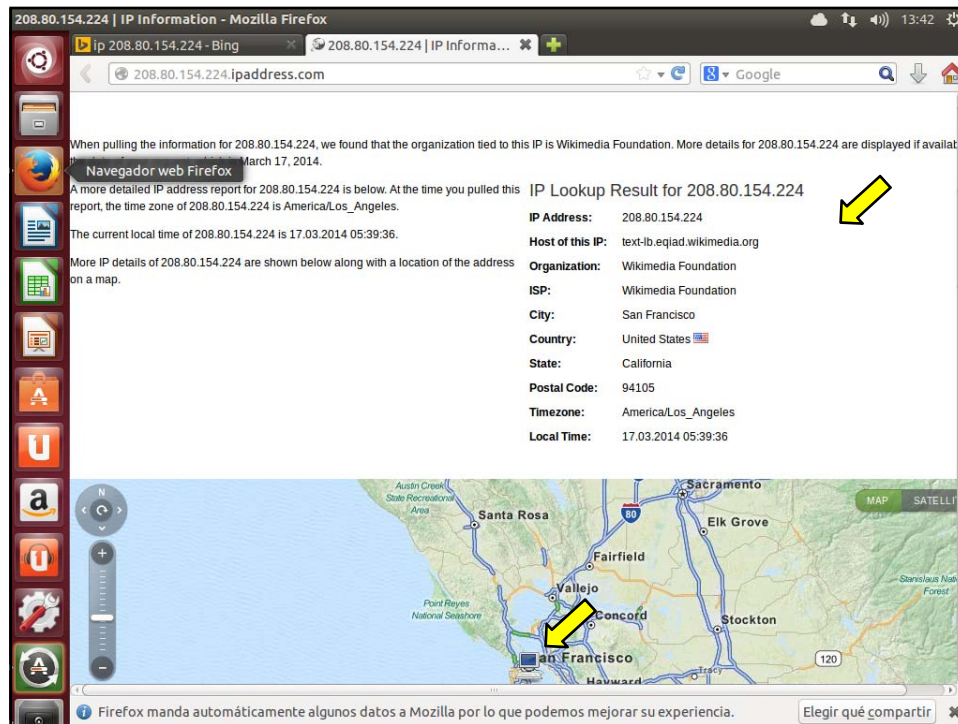
## Utilidad nslookup

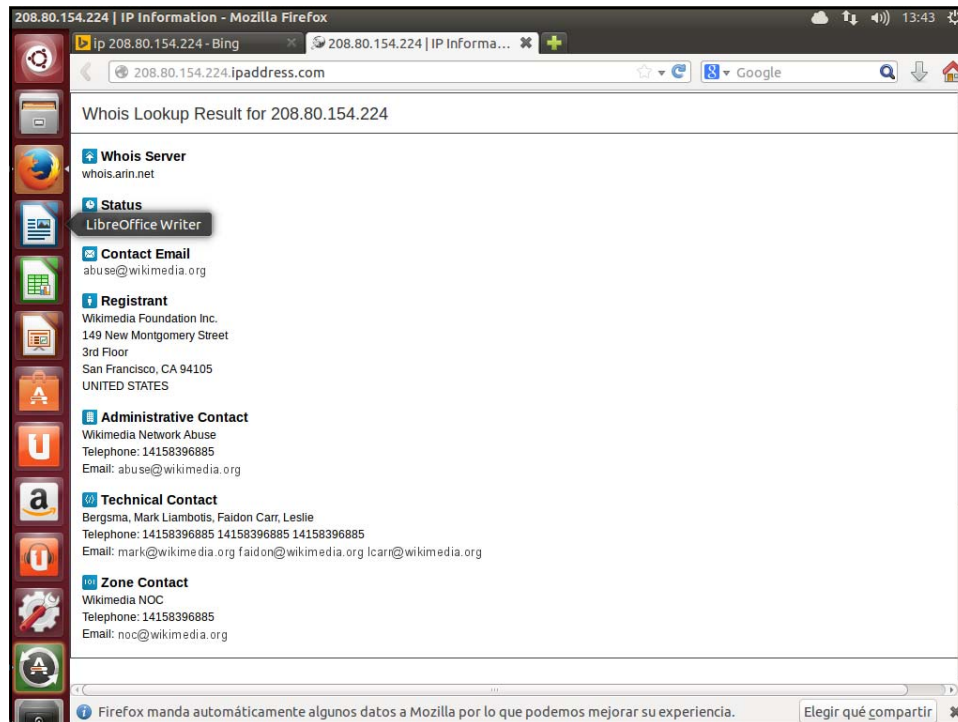
```
labadmin@ub32: ~  
labadmin@ub32:~$ nslookup wikipedia.com  
Server: 127.0.1.1  
Address: 127.0.1.1#53  
Non-authoritative answer:  
Name: wikipedia.com  
Address: 208.80.154.224  
labadmin@ub32:~$ nslookup wikipedia.org  
Server: 127.0.1.1  
Address: 127.0.1.1#53  
Non-authoritative answer:  
Name: wikipedia.org  
Address: 208.80.154.224  
labadmin@ub32:~$
```



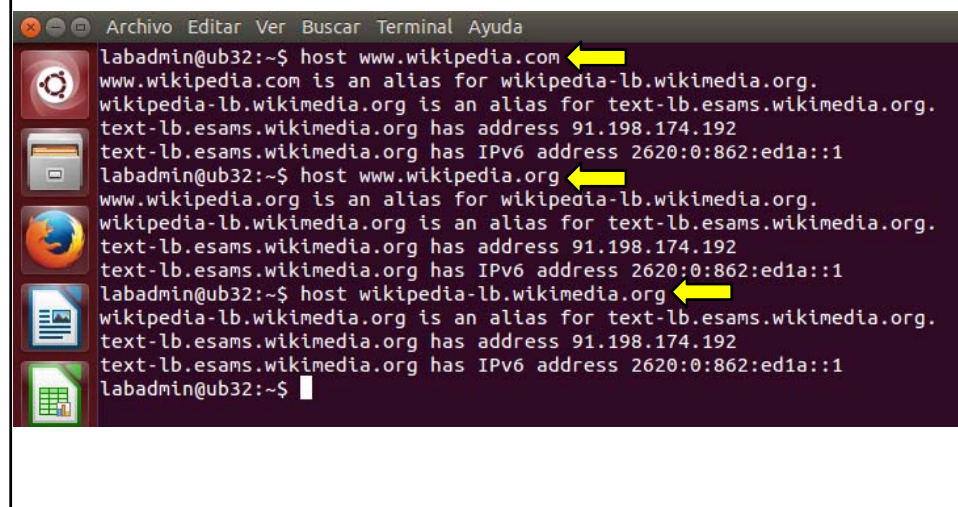
## Búsqueda de IP en BING para geolocalización (varias diapos)







## Utilidad host





## Ejemplo de host con IP múltiple (www.google.com)

```
labadmin@ub32: ~  
labadmin@ub32:~$ host www.google.com  
www.google.com has address 173.194.34.209  
www.google.com has address 173.194.34.208  
www.google.com has address 173.194.34.211  
www.google.com has address 173.194.34.212  
www.google.com has address 173.194.34.210  
www.google.com has IPv6 address 2a00:1450:4003:801::1011  
labadmin@ub32:~$  
labadmin@ub32:~$ host www.google.es  
www.google.es has address 173.194.34.223  
www.google.es has address 173.194.34.215  
www.google.es has address 173.194.34.216  
www.google.es has IPv6 address 2a00:1450:4003:801::1017  
labadmin@ub32:~$
```

Parte segunda:

## ESTUDIO DE NSLOOKUP

## **Estudio de nslookup para Windows**

- Estudia la página  
<http://norfipc.com/redes/como-usar-comando-nslookup-windows.html>
- Practica con un sistema Windows la herramienta nslookup

## **Estudio de nslookup para Ubuntu**

- Repite el estudio de nslookup pero ahora para un sistema Ubuntu o similar
- Tendrás que buscar información en Internet sobre la implementación concreta de nslookup para la distribución GNU/Linux que utilices para hacer el estudio

## Para hacer

- Elige una empresa que tenga una importancia relevante en Internet
  - Por ejemplo, Facebook, Twitter, Amazon, Google, etc.
    - Elige otra distinta que no sea ninguna del ejemplo anterior
- Ejecuta las utilidades estudiadas para averiguar todo lo que puedas de esas empresas a partir de la información pública que está accesible en Internet

## Para entregar

- Una vez finalizada la práctica deberás entregar:
  - El informe de práctica con los detalles de ejecución según la plantilla de prácticas
  - Un manual de nslookup para Windows
  - Un manual de nslookup para GNU/Linux
  - Un informe con toda la información conseguida sobre la compañía en Internet de tu elección y los medios utilizados para conseguir cada dato
- Nomenclatura identificativa de práctica:
  - **PARP409-InforDominios**