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

Alfredo Abad

UA: 13-ago-2018

PARP409-InforDominios.pptx

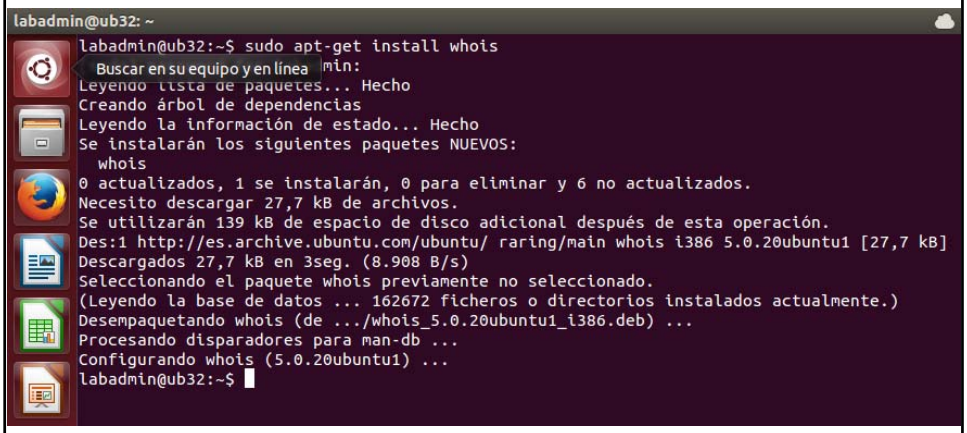
Objetivo

- 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

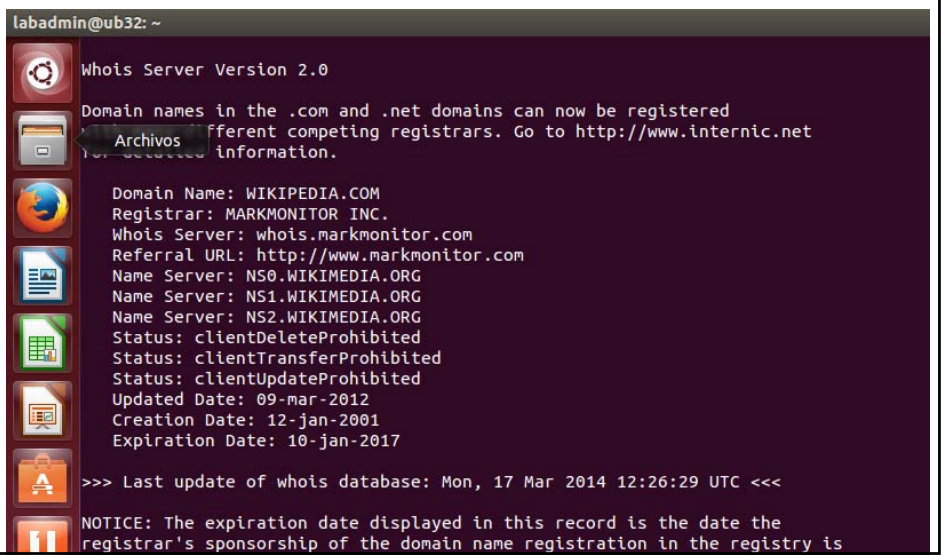
Parte primera:

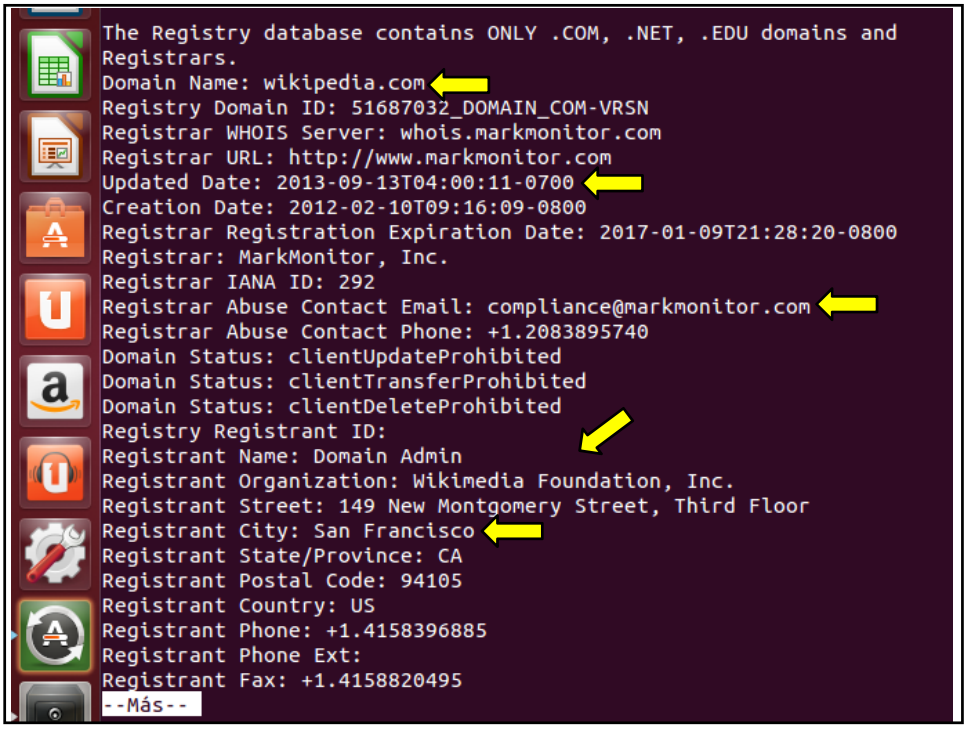
ESTUDIO GENERAL DE ALGUNAS UTILIDADES

Herramienta whois (comenzamos instalando whois)

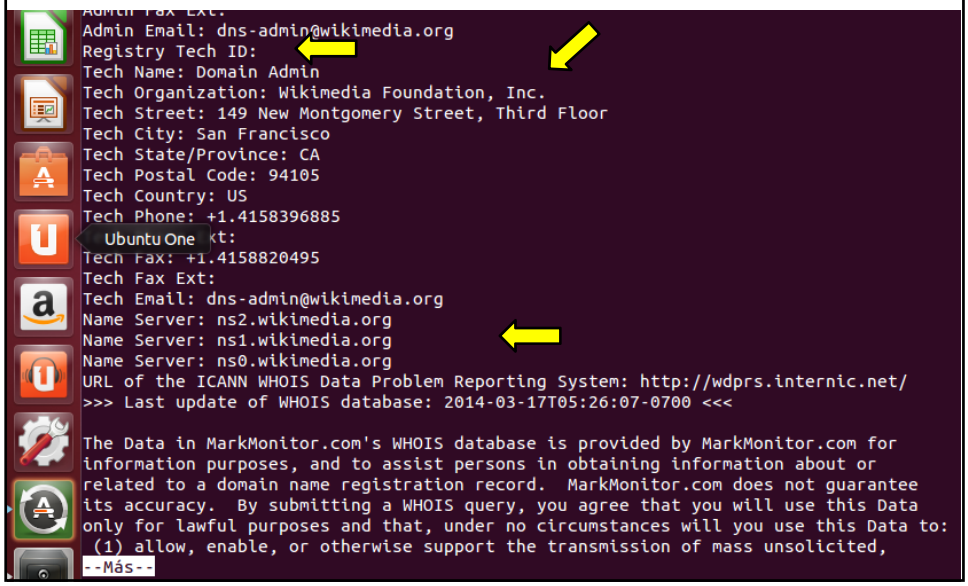


Ejecución de whois wikipedia.com (varias diapos)

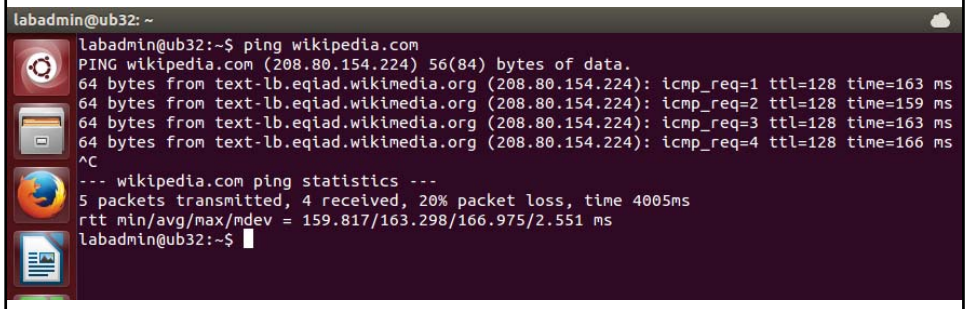




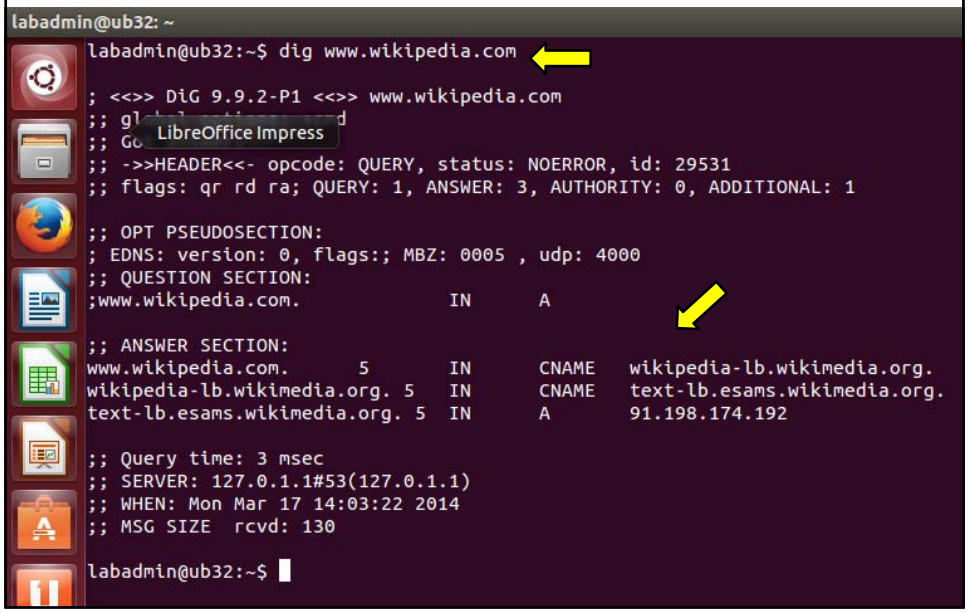
Administrador técnico y DNS



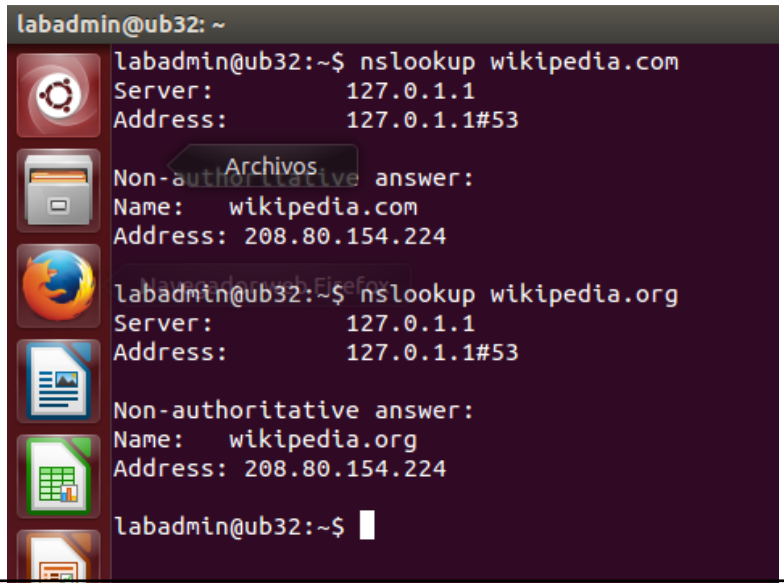
Conseguir una IP del dominio (se puede hacer utilizando la resolución que disparará ping)



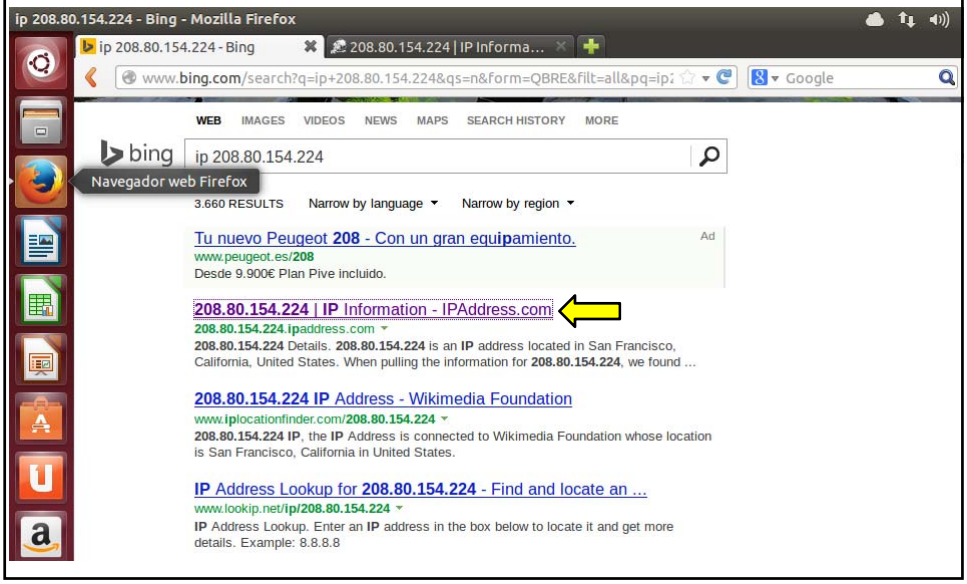
Utilidad dig

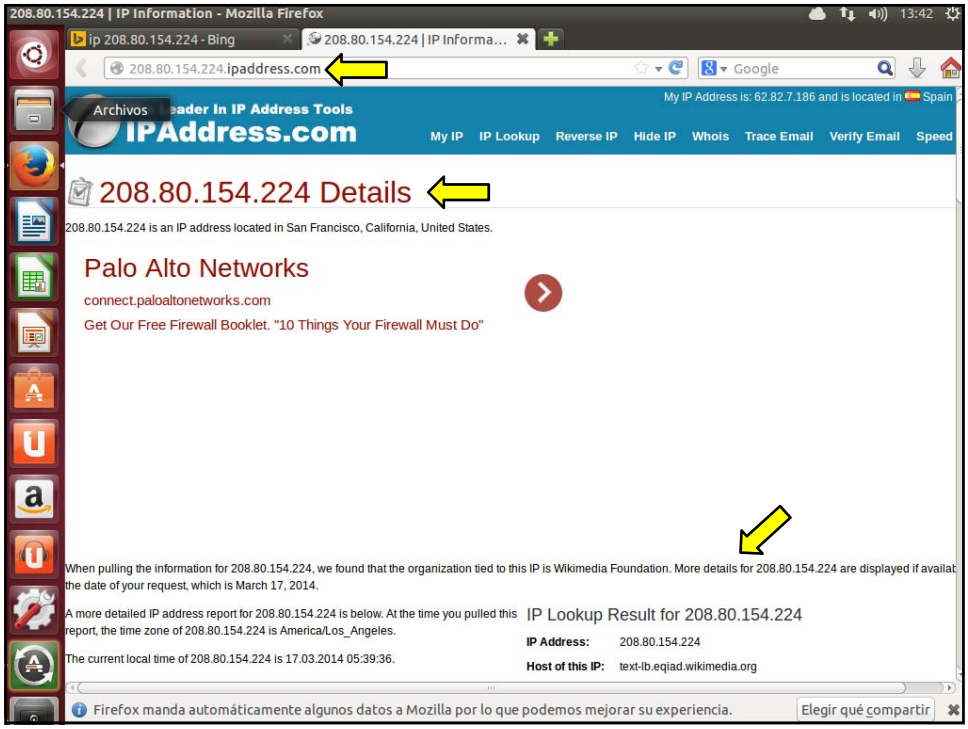


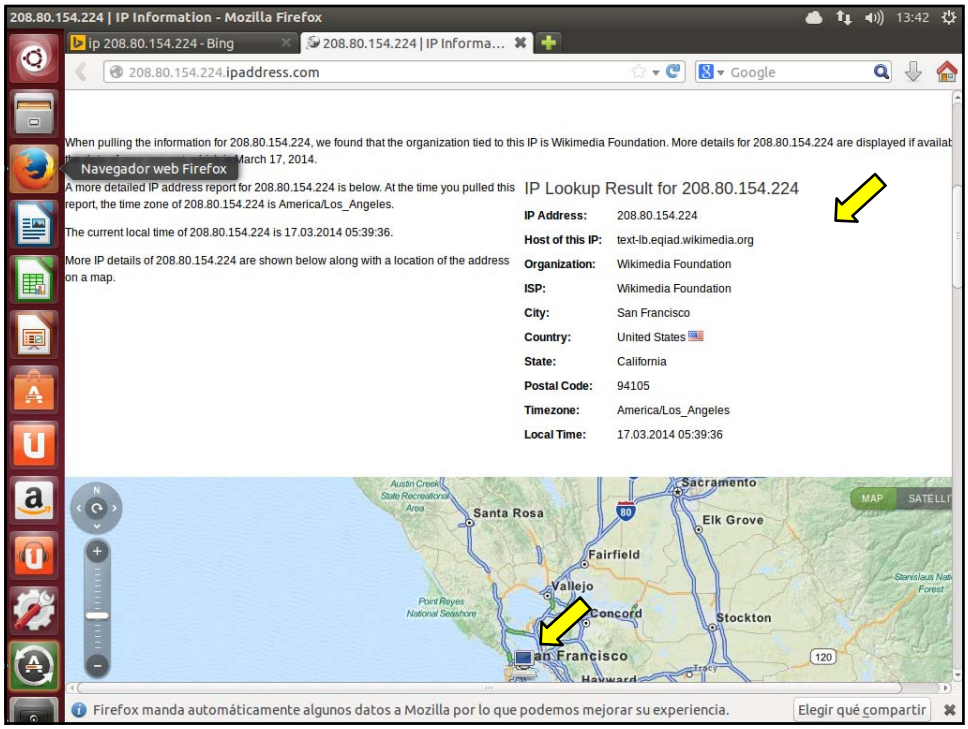
Utilidad nslookup

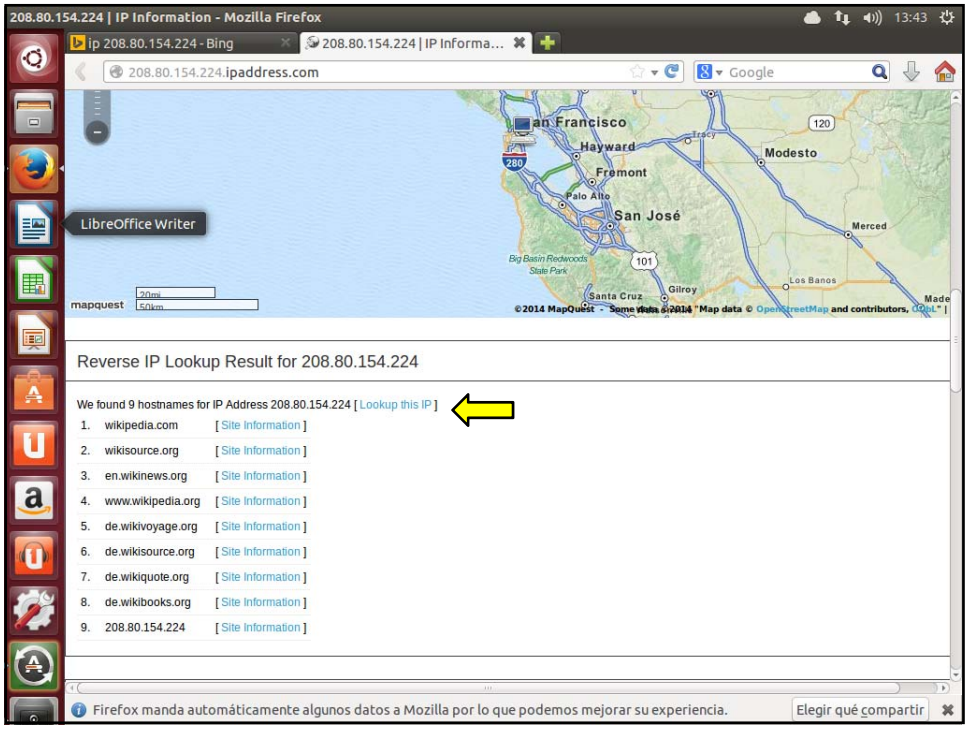


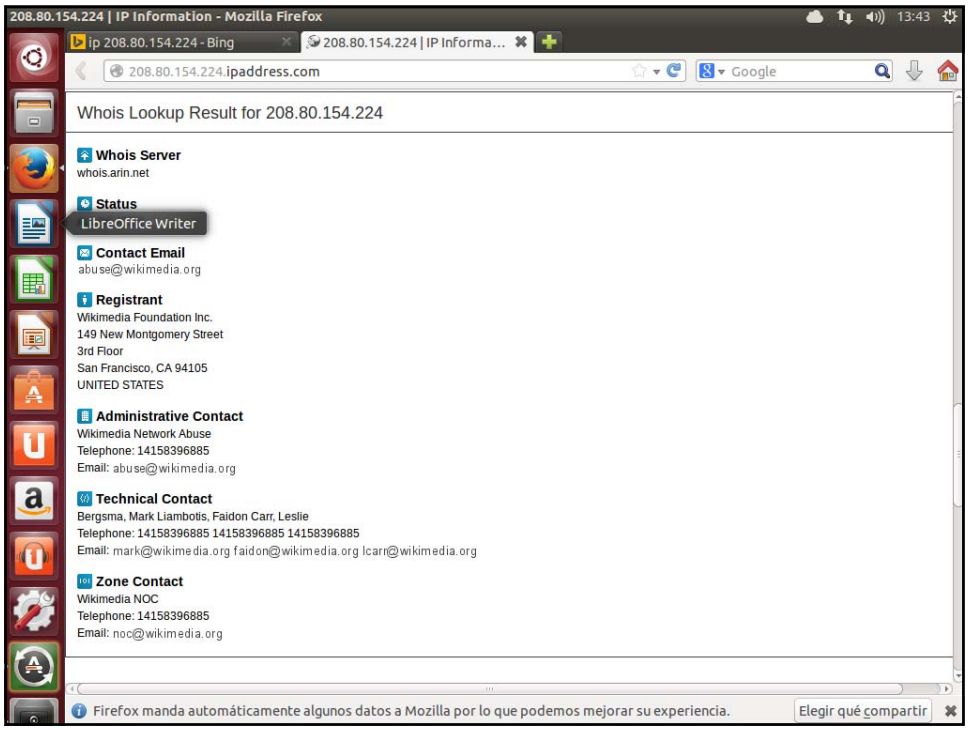
Búsqueda de IP en BING para geolocalización (varias diapos)



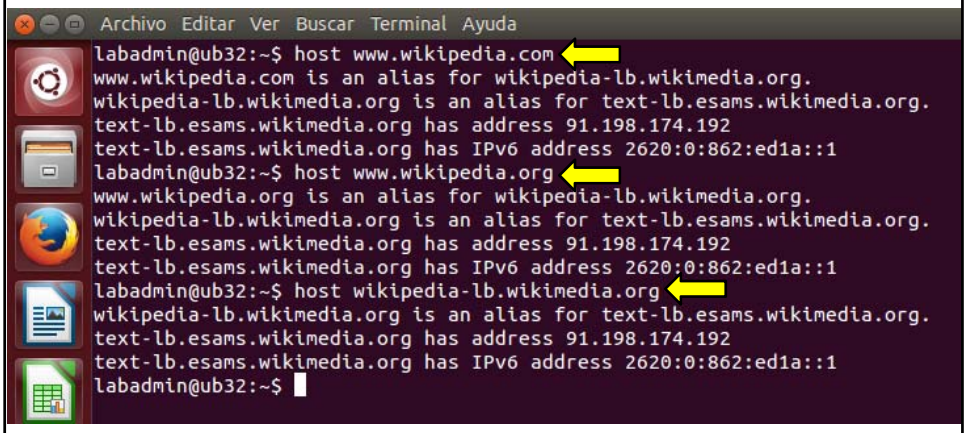



208.80.154.224 | IP Information - Mozilla Firefox
13:42
ip 208.80.154.224 - Bing
208.80.154.224 | IP Informa...
208.80.154.224.ipaddress.com
Google
Navegador web Firefox
When pulling the information for 208.80.154.224, we found that the organization tied to this IP is Wikimedia Foundation. More details for 208.80.154.224 are displayed if availat
March 17, 2014.
A more detailed IP address report for 208.80.154.224 is below. At the time you pulled this report, the time zone of 208.80.154.224 is America/Los_Angeles.
The current local time of 208.80.154.224 is 17.03.2014 05:39:36.
More IP details of 208.80.154.224 are shown below along with a location of the address on a map.
IP Lookup Result for 208.80.154.224
IP Address: 208.80.154.224
Host of this IP: text-lb.eqiad.wikimedia.org
Organization: Wikimedia Foundation
ISP: Wikimedia Foundation
City: San Francisco
Country: United States
State: California
Postal Code: 94105
Timezone: America/Los_Angeles
Local Time: 17.03.2014 05:39:36
Sacramento
Santa Rosa
Elk Grove
Fairfield
Vallejo
Concord
Stockton
San Francisco
Hayward
MAP
Firefox manda automáticamente algunos datos a Mozilla por lo que podemos mejorar su experiencia.
Elegir qué compartir

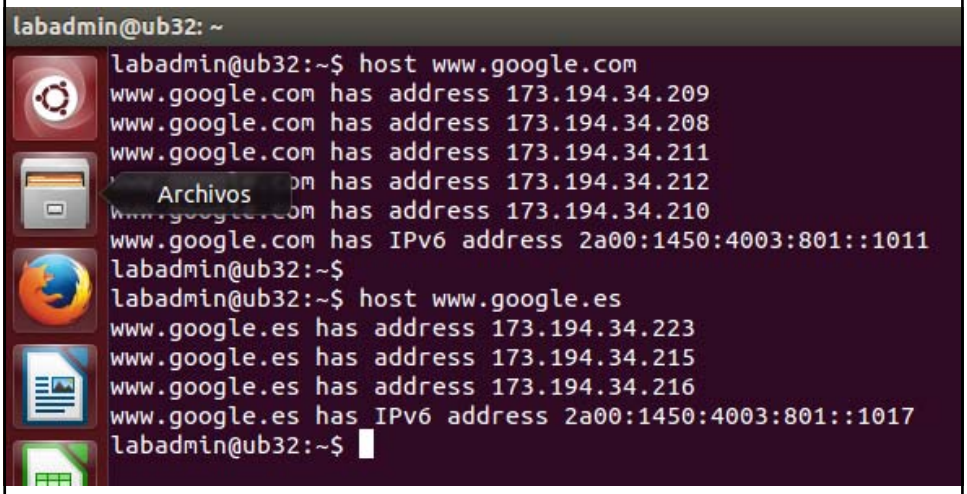

208.80.154.224 | IP Information - Mozilla Firefox
13:43
ip 208.80.154.224 - Bing
208.80.154.224 | IP Informa...
208.80.154.224.ipaddress.com
Google
LibreOffice Writer
San Francisco
Hayward
Fremont
Palo Alto
San José
Modesto
Merced
Santa Cruz
Gilroy
Los Banos
mapquest
Reverse IP Lookup Result for 208.80.154.224
We found 9 hostnames for IP Address 208.80.154.224 [Lookup this IP]
1. wikipedia.com [Site Information]
2. wikisource.org [Site Information]
3. en.wikinews.org [Site Information]
4. www.wikipedia.org [Site Information]
5. de.wikivoyage.org [Site Information]
6. de.wikisource.org [Site Information]
7. de.wikiquote.org [Site Information]
8. de.wikibooks.org [Site Information]
9. 208.80.154.224 [Site Information]
Firefox manda automáticamente algunos datos a Mozilla por lo que podemos mejorar su experiencia.
Elegir qué compartir



Utilidad host



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



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 nslooup 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**