

# Práctica 3

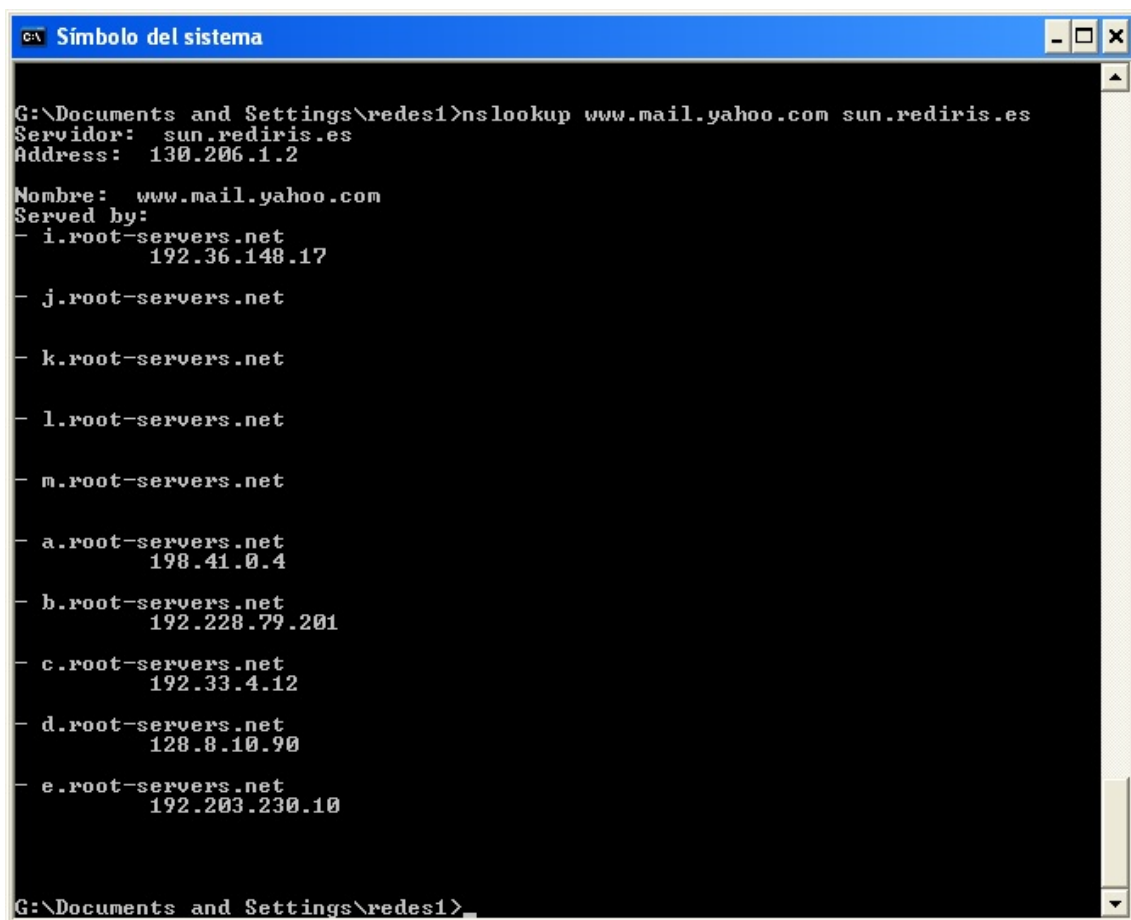
## Redes de Computadores

David Morales Sáez  
Alberto Manuel Mireles Suárez

## 1. nslookup

1. La dirección de la web china: [www.taobao.com](http://www.taobao.com) es, según el nslookup: 119.167.201.241.
2. Los servidores DNS autoritativos para la web de la Universidad Politécnica de Cataluña ([www.upc.es](http://www.upc.es)) son los siguientes:

sun.rediris.es	130.206.1.2
chico.rediris.es	130.206.1.3
euler.upc.es	147.83.2.10
buckus.upc.es	147.83.2.3
3. Al preguntarle a uno de los servidores DNS por los servidores email de Yahoo obtenemos lo siguiente:



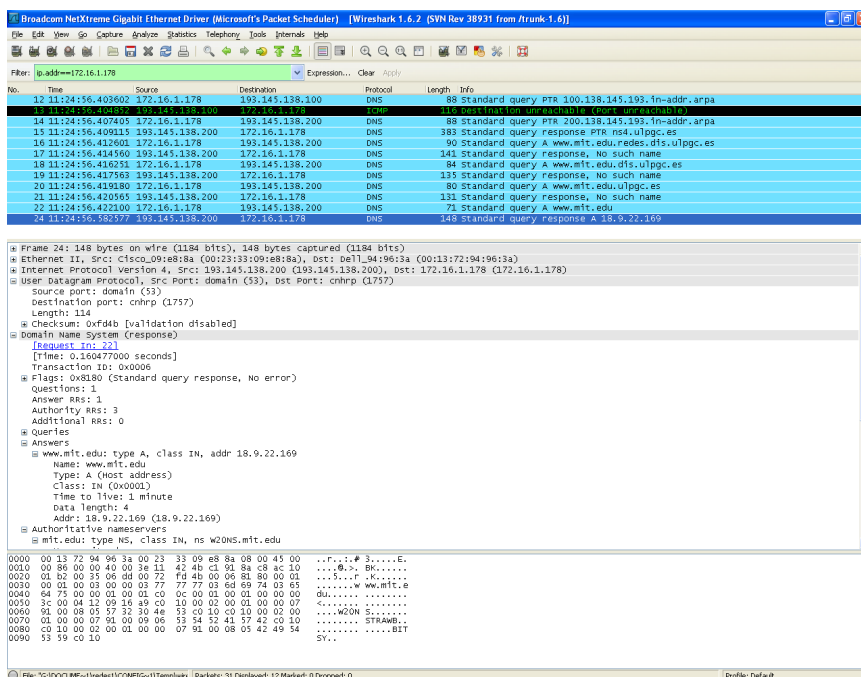
```
G:\Documents and Settings\redes1>nslookup www.mail.yahoo.com sun.rediris.es
Servidor: sun.rediris.es
Address: 130.206.1.2

Nombre: www.mail.yahoo.com
Served by:
- i.root-servers.net
    192.36.148.17
- j.root-servers.net
- k.root-servers.net
- l.root-servers.net
- m.root-servers.net
- a.root-servers.net
    198.41.0.4
- b.root-servers.net
    192.228.79.201
- c.root-servers.net
    192.33.4.12
- d.root-servers.net
    128.8.10.90
- e.root-servers.net
    192.203.230.10

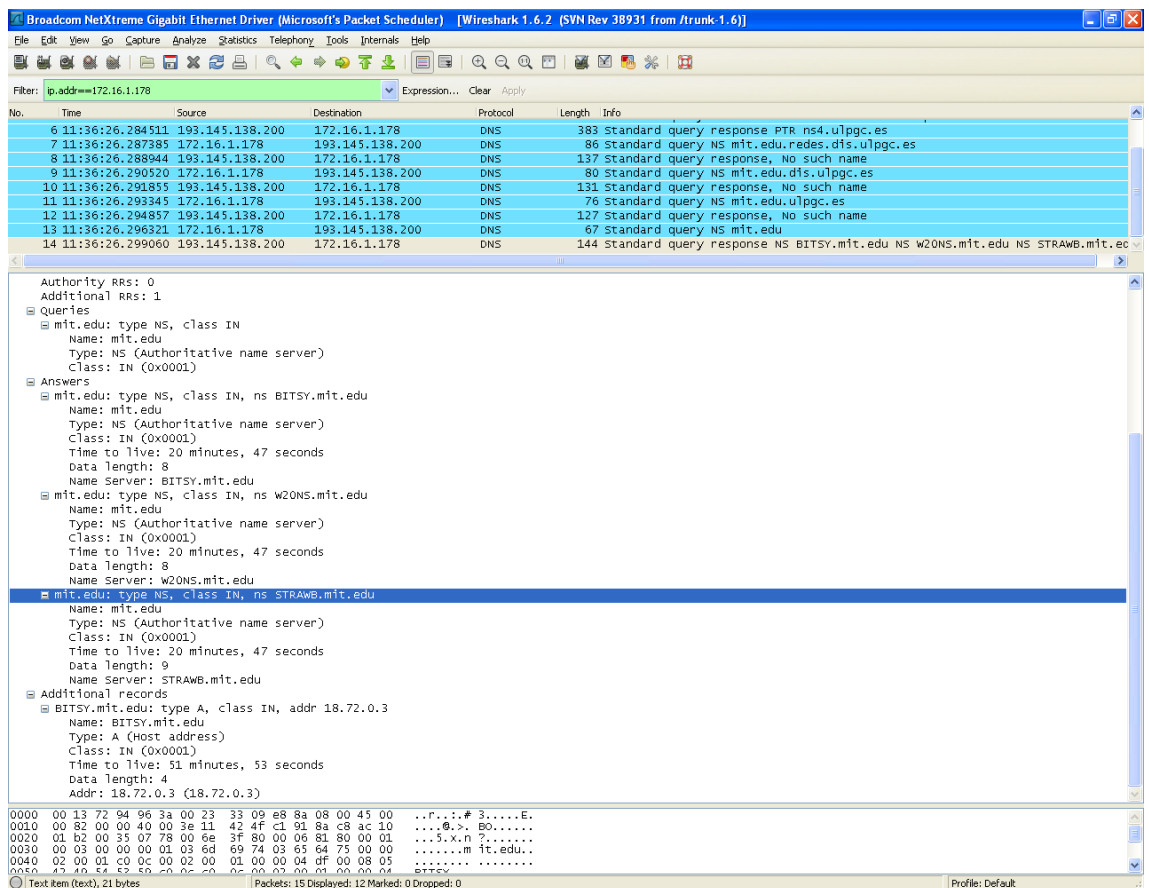
G:\Documents and Settings\redes1>
```

### 3. Tracing DNS with Wireshark

- Las peticiones de DNS se envían sobre UDP.
- Los puertos de origen y destino para las peticiones de DNS son los mismos, el puerto 53.
- El query message se envía a la IP 172.16.1.178. Esta IP coincide con la dirección de nuestro servidor DNS local.
- El tipo de la petición DNS es A (host adress) y a su vez, contiene una respuesta.
- Al examinar la respuesta de la petición DNS, observamos que hay una respuesta que contiene: el nombre, el tipo, la clase, el tiempo de vida, el tamaño de los datos y la dirección.
- Si, la IP de destino coincide con una IP que figura en la respuesta del mensaje, que es: 12.22.58.30.
- No, al recuperar cada imagen, no hace nuevas peticiones de DNS.
- Tanto el puerto de destino de la solicitud DNS como el puerto de origen de la respuesta DNS es 53.
- La solicitud DNS se ha enviado a la dirección 172.16.1.178, mientras que nuestro servidor DNS local tiene la dirección 193.145.138.200.
- La solicitud DNS es de tipo A (Dirección del Host), y no tiene ningún tipo de respuesta.
- La respuesta DNS tiene una respuesta, que tiene lo siguiente  
www.mit.edu: type A, class IN, addr 18.9.22.169  
Name: www.mit.edu  
Type: A (Host Address)  
Class: IN (0x0001)  
Time to live: 1 minute  
Data length: 4  
Addr: 18.9.22.169 (18.9.22.169)
- 15.



16. El mensaje DNS se envió a la dirección IP 172.16.1.178. No, ya que nuestra dirección es 193.145.138.200.
  17. La solicitud DNS es del tipo “NS” (Authorative name server) y no contiene ningún tipo de respuesta.
  18. El mensaje de la respuesta tiene los siguientes nombres de servidor:
    - a. BITSY.mit.edu
    - b. w20ns.mit.edu
    - c. STRAWB.mit.edu
- El mensaje no incluye las direcciones IP de los servidores.
- 19.



20. El mensaje ha sido enviado a la dirección IP 172.16.1.178, y corresponde a 193.145.138.100.
21. La solicitud DNS es del tipo “A” (Dirección del Host) y sí, contiene una respuesta.
22. La respuesta a la solicitud contiene una respuesta, que es la siguiente:
  - bitsy.mit.edu: type A, class IN, addr 18.72.0.3
  - Name: bitsy.mit.edu
  - Type: A (Host Address)
  - Class: IN (0x0001)
  - Time to live: 56 minutes, 59 seconds
  - Data length: 4
  - Addr: 18.72.0.3 (18.72.0.3)

23.

Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) [Wireshark 1.6.2 (SVN Rev 38931 from trunk 1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr==172.16.1.178 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
6	11:42:37.548661	172.16.1.178	193.145.138.100	DNS	73	Standard query A bitsy.mt.edu
7	11:42:37.550163	193.145.138.100	172.16.1.178	DNS	144	Standard query response A 18.72.0.3
8	11:42:37.555801	172.16.1.178	18.72.0.3	DNS	82	Standard query PTR 3.0.72.18.in-addr.arpa
10	11:42:37.700788	18.72.0.3	172.16.1.178	DNS	212	Standard query response PTR bitsy.mt.edu
11	11:42:37.703775	172.16.1.178	18.72.0.3	DNS	93	Standard query A www.aft.or.kr.redes.dfs.ulpgc.es
12	11:42:37.849293	18.72.0.3	172.16.1.178	DNS	144	Standard query response, No such name
13	11:42:37.850919	172.16.1.178	18.72.0.3	DNS	87	Standard query A www.aft.or.kr.dfs.ulpgc.es
14	11:42:38.154981	18.72.0.3	172.16.1.178	DNS	138	Standard query response, No such name
15	11:42:38.157084	172.16.1.178	18.72.0.3	DNS	83	Standard query A www.aft.or.kr.ulpgc.es
16	11:42:38.602007	18.72.0.3	172.16.1.178	DNS	134	Standard query response, No such name
17	11:42:38.603763	172.16.1.178	18.72.0.3	DNS	74	Standard query A www.aft.or.kr
18	11:42:38.748968	18.72.0.3	172.16.1.178	DNS	124	Standard query response A 121.254.171.27

Frame 7: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)

- Ethernet II, Src: cisco.09:e8:8a (00:23:33:09:e8:8a), Dst: dell.94:96:3a (00:13:72:94:96:3a)
- Internet Protocol Version 4, Src: 193.145.138.100 (193.145.138.100), Dst: 172.16.1.178 (172.16.1.178)
- User Datagram Protocol, Src Port: domain (53), Dst Port: 65017 (65017)
  - Source port: domain (53)
  - Destination port: 65017 (65017)
  - Length: 110
  - Checksum: 0xc705 [validation disabled]
- Domain Name System (response)
  - Request ID: 6
  - Time: 0.001502000 seconds
  - Transaction ID: 0x7510
  - Flags: 0x8180 (Standard query response, No error)
  - Questions: 1
    - Answer RRs: 1
    - Authority RRs: 3
    - Additional RRs: 0
  - Queries
    - bitsy.mt.edu: type A, class IN
      - Name: bitsy.mt.edu
      - Type: A (Host address)
      - Class: IN (0x0001)
  - Answers
    - bitsy.mt.edu: type A, class IN, addr 18.72.0.3
      - Name: bitsy.mt.edu
      - Type: A (Host address)
      - Class: IN (0x0001)
      - Time to live: 56 minutes, 59 seconds
      - Data length: 4
      - Addr: 18.72.0.3 (18.72.0.3)
  - Authoritative nameservers

0000 00 13 72 94 96 3a 00 23 33 09 e8 8a 08 00 45 00 ...r...i.# 3.....E.  
0010 00 82 00 00 40 00 3e 11 42 b3 c1 91 8a 64 ac 10 ...0>. 8....d..  
0020 02 b3 00 35 fd f9 00 6a c7 05 75 10 82 80 00 01 ...5...n ...u....  
0030 00 02 00 03 00 00 05 62 69 74 73 79 03 6d 69 74 .....b ttsy.mt  
0040 03 63 64 73 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu... ..  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

File: %DOCUMENT%\Index\CONFIG-1\Temp\ Packets: 20 Displayed: 12 Marked: 0 Dropped: 0 Profile: Default