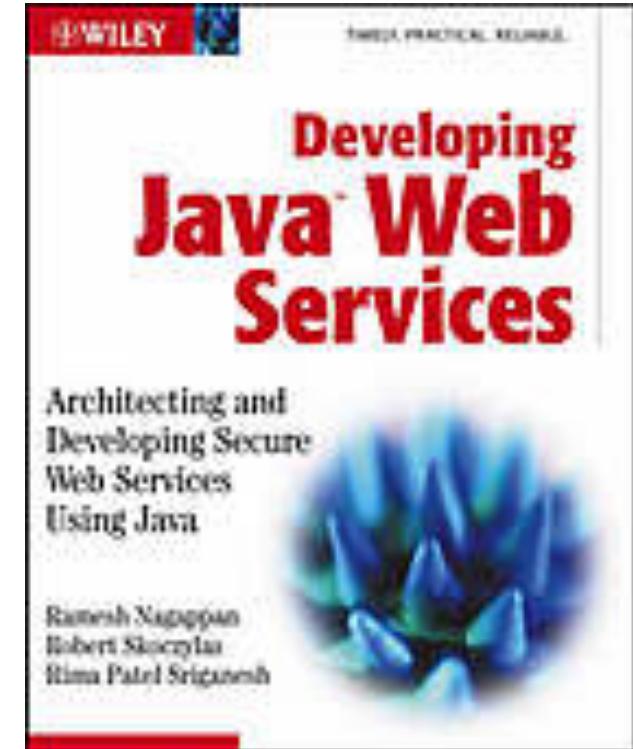
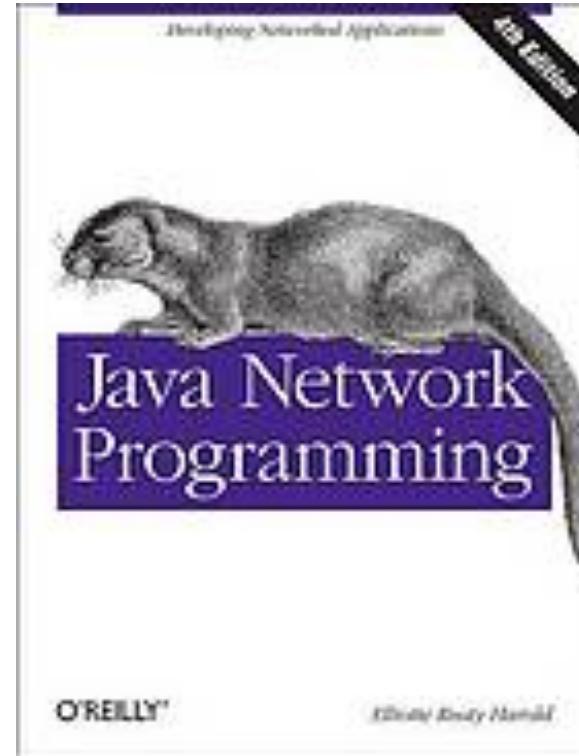
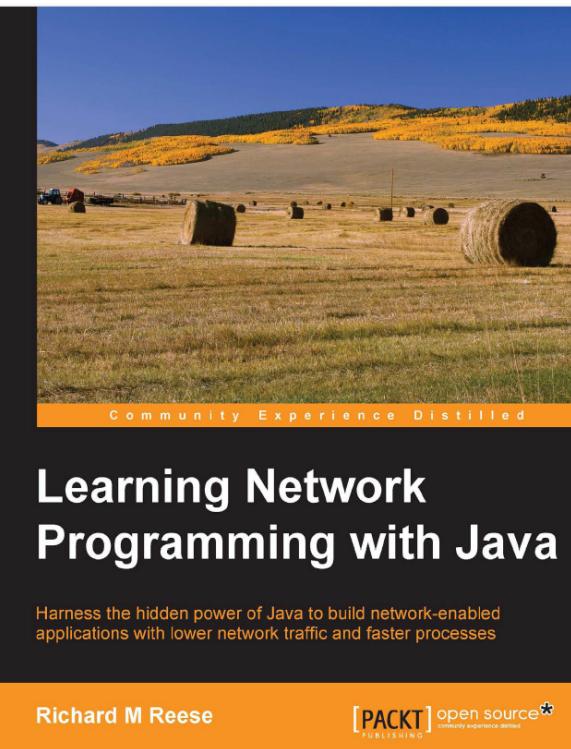
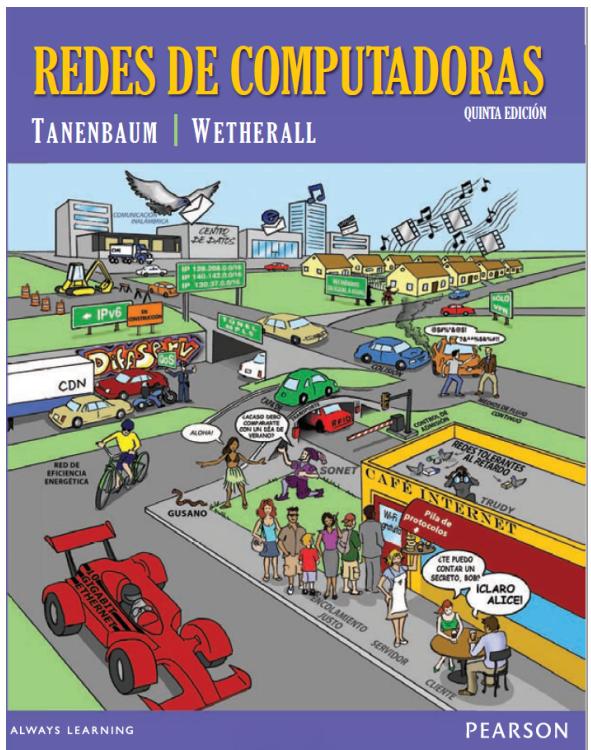


# **REDES DE COMPUTADORES Y LABORATORIO**

**Yor Castaño, MSc**



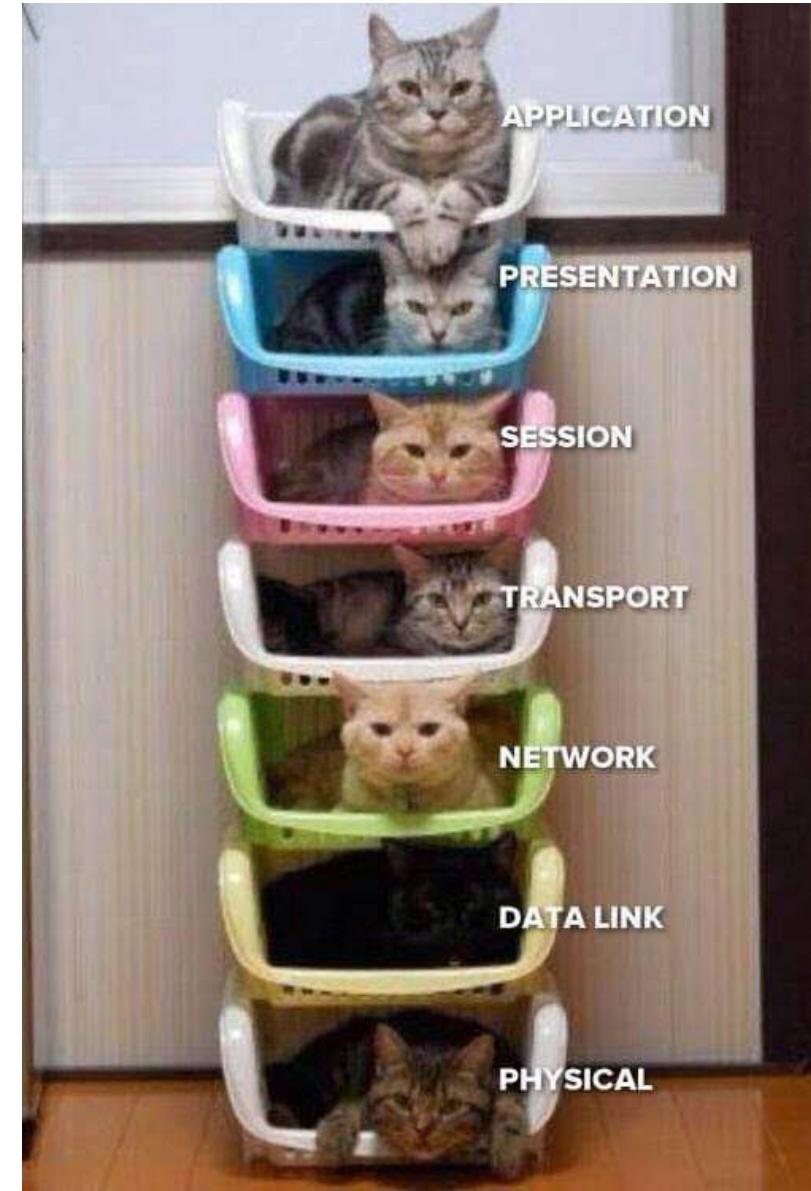
# BIBLIOGRAFÍA



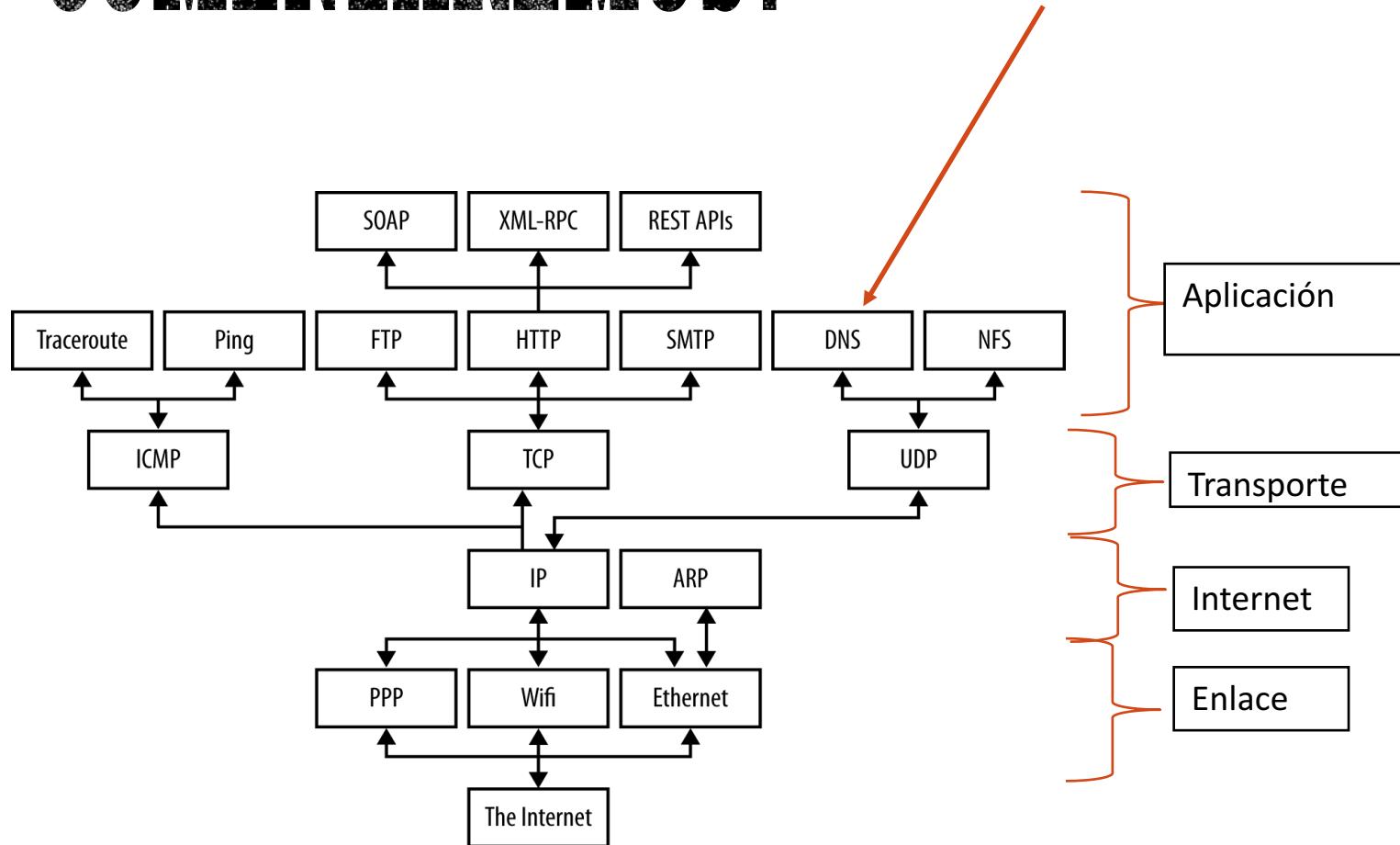
# COMPETENCIAS

- Describir la capa de aplicación.
  - Describir DNS
  - Describir correo electrónico.
  - Describir World Wide Web
    - Páginas estáticas
    - Páginas dinámicas

# LA CAPA DE APLICACIÓN



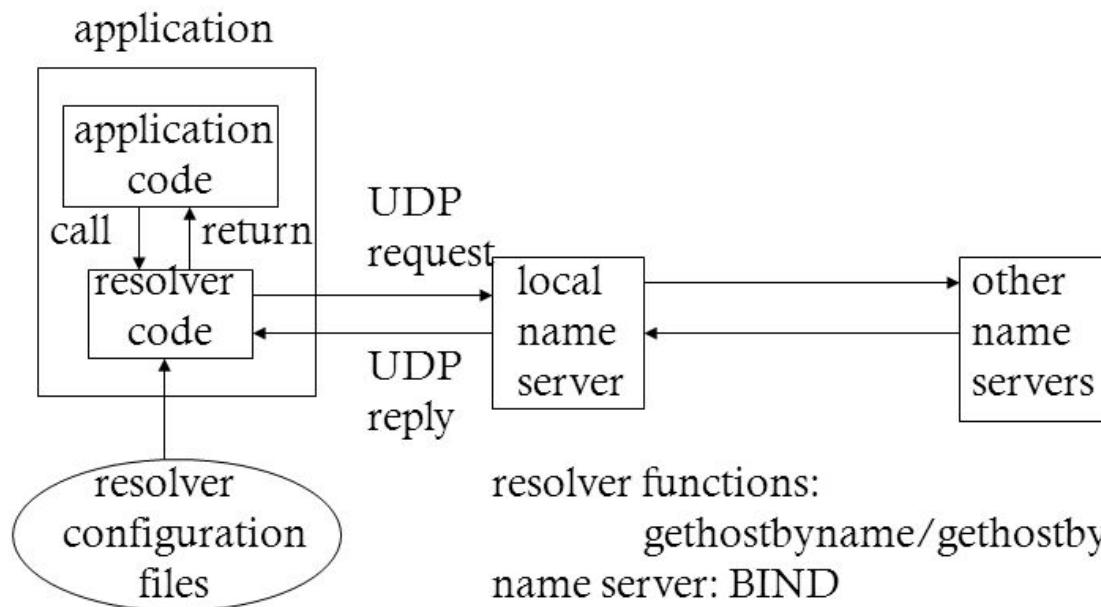
# DÓNDE COMENZAREMOS?



# DNS: EL SISTEMA DE NOMBRES DE DOMINIO

- Como hemos visto, nosotros podemos hacer una comunicación entre host a través de su dirección IP, pero es muy difícil recordar un número en notación decimal para todos los involucrados en una red de computadoras.
  - Además, si una compañía mueve su servidor web a una máquina distinta tendría que avisar a todos los nodos el nuevo cambio.
- Anteriormente existía un archivo *host.txt* donde se listaban las direcciones IP y los nombres de computadoras.
- **En 1983 se inventó el DNS (Domain Name System), parte clave de Internet desde entonces.**
- DNS es un esquema jerárquico de nombres basado en dominios y un sistema de base de datos distribuido. ([RFC 1034](#), [1035](#), [2181](#))

# DNS: Application, Resolver, Name Servers



## **Resolución de nombres**

resolver functions:

gethostbyname/gethostbyaddr

name server: BIND

(Berkeley Internet Name Domain)

static hosts files (DNS alternatives):

/etc/hosts

resolver configuration file (specifies name server IPs):

/etc/resolv.conf

# DNS: EL SISTEMA DE NOMBRES DE DOMINIO

- Internet se divide en 250 **dominios de nivel superior**. Existen dos categorías: genéricos y países.
- Cada dominio se divide en subdominios.
- La práctica de registrar un dominio con miras a venderlo después a una parte interesada a un precio mucho mayor se conoce como: **ciberocupación (cybersquatting)**.

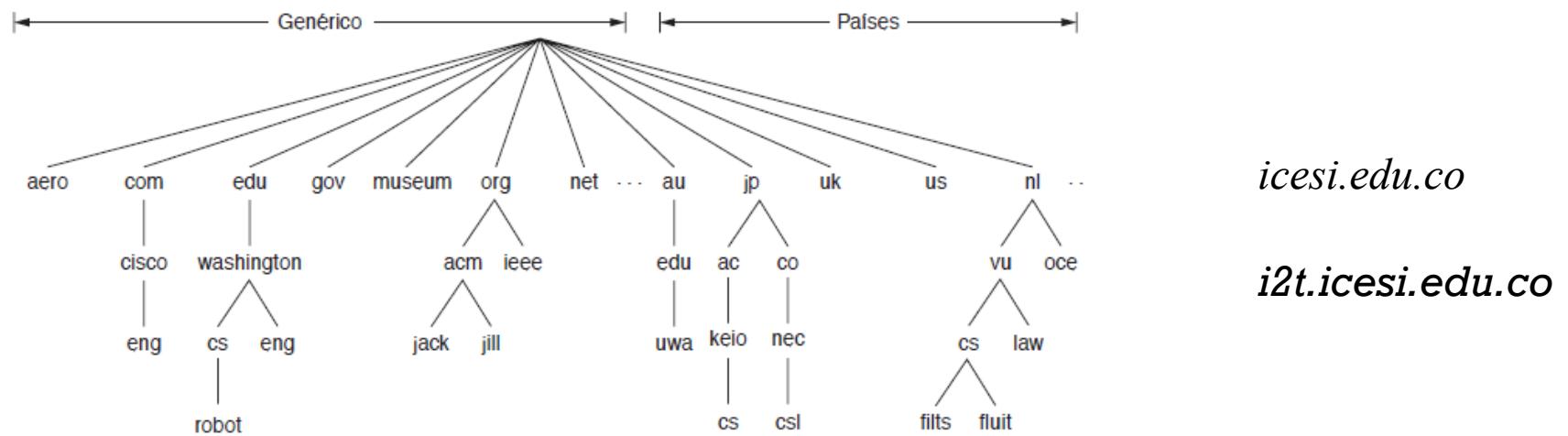


Figura 7-1. Una porción del espacio de nombres de dominio de Internet.

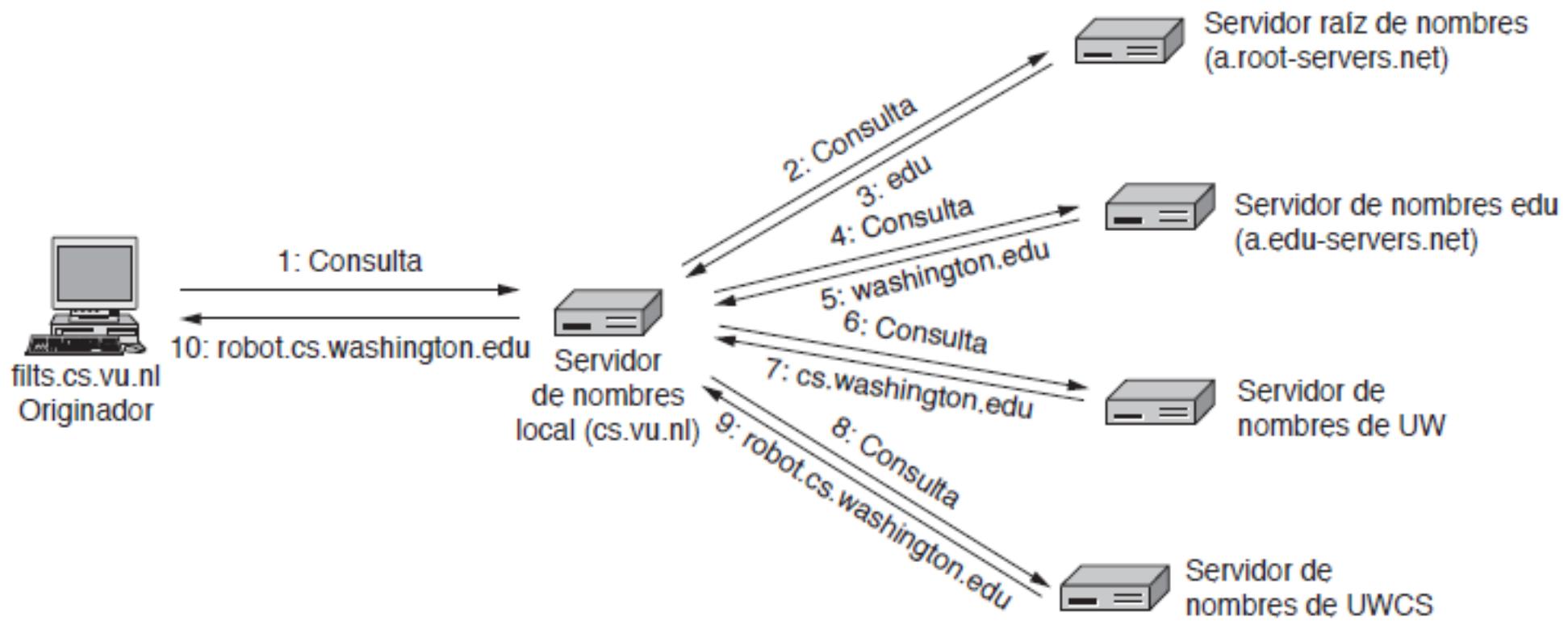
# DNS: EL SISTEMA DE NOMBRES DE DOMINIO

- Cada dominio de nivel superior, puede tener un grupo de **registros de recursos** asociados a él.
- Cuando un **solucionador/cliente** asigna un nombre de dominio al DNS, lo que recibe son las variables de los recursos asociados a ese nombre.

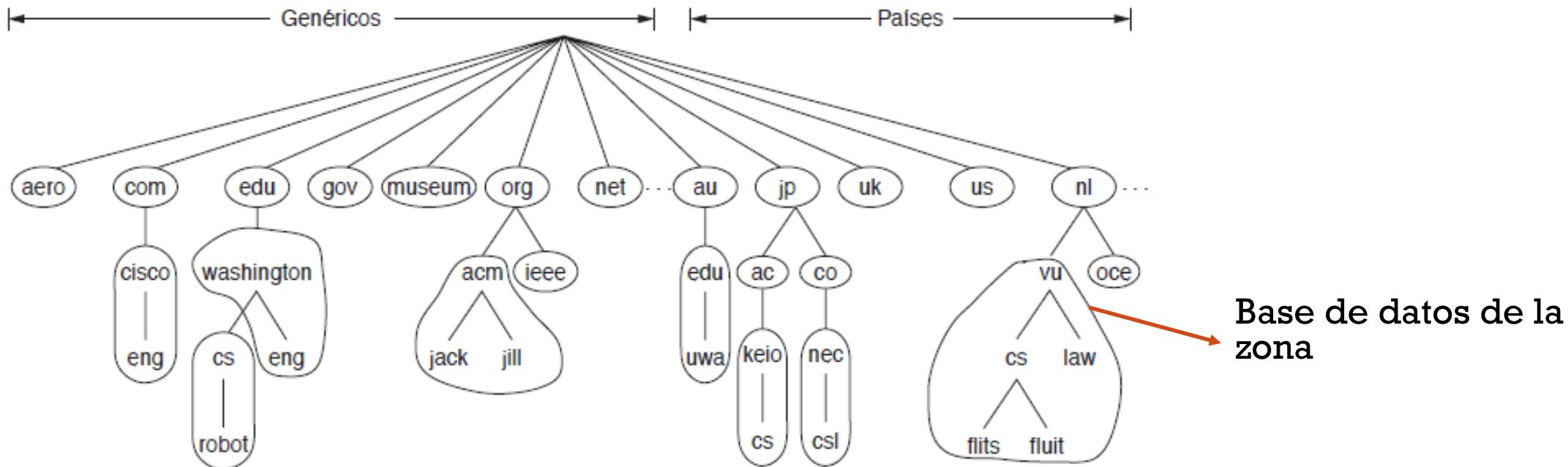
| <i>Nombre_dominio</i>              | <i>Tiempo_de_vida</i>                   | <i>Clase</i>   | <i>Tipo</i> | <i>Valor</i>                                |
|------------------------------------|---|--|-------------|---|
| Tipo                               | Significado                             | Valor  |             |   |
| SOA                                | Inicio de autoridad                     | Parámetros para esta zona.                                 |             |   |
| A                                  | Dirección IPv4 de un host               | Entero de 32 bits.   |             |   |
| AAAA                               | Dirección IPv6 de un host               | Entero de 128 bits.  |             |   |
| MX                                 | Intercambio de correo                   | Prioridad, dominio dispuesto a aceptar correo electrónico. |             |   |
| NS                                 | Servidor de nombres                     | Nombre de un servidor para este dominio.                   |             |   |
| CNAME                              | Nombre canónico                         | Nombre de dominio.   |             |   |
| PTR                                | Apuntador                               | Alias de una dirección IP.                                 |             |   |
| SPF                                | Marco de trabajo de política del emisor | Codificación de texto de la política de envío de correo.   |             |   |
| SRV                                | Servicio                                | Host que lo provee.  |             |   |
| TXT                                | Texto                                   | Texto ASCII descriptivo.                                   |             |   |
| ; Datos autoritarios para cs.vu.nl |   |  |             |   |
| cs.vu.nl.                          | 86400                                   | IN   | SOA         | star boss (9527, 7200, 7200, 241920, 86400) |
| cs.vu.nl.                          | 86400                                   | IN   | MX          | 1 zephyr                                    |
| cs.vu.nl.                          | 86400                                   | IN   | MX          | 2 top                                       |
| cs.vu.nl.                          | 86400                                   | IN   | NS          | star  |
| star                               | 86400                                   | IN   | A           | 130.37.56.205                               |
| zephyr                             | 86400                                   | IN   | A           | 130.37.20.10                                |
| top                                | 86400                                   | IN   | A           | 130.37.20.11                                |
| www                                | 86400                                   | IN   | CNAME       | star.cs.vu.nl                               |
| ftp                                | 86400                                   | IN   | CNAME       | zephyr.cs.vu.nl                             |
| flits                              | 86400                                   | IN   | A           | 130.37.16.112                               |
| flits                              | 86400                                   | IN   | A           | 192.31.231.165                              |
| flits                              | 86400                                   | IN   | MX          | 1 flits                                     |
| flits                              | 86400                                   | IN   | MX          | 2 zephyr                                    |
| flits                              | 86400                                   | IN   | MX          | 3 top                                       |
| rowboat                            |   | IN   | A           | 130.37.56.201                               |
|                                    |   | IN   | MX          | 1 rowboat                                   |
|                                    |   | IN   | MX          | 2 zephyr                                    |
| little-sister                      |   | IN   | A           | 130.37.62.23                                |
| laserjet                           |   | IN   | A           | 192.31.231.216                              |

Figura 7-3. Los principales tipos de registros de recursos de DNS.

Figura 7-4. Parte de una posible base de datos DNS para cs.vu.nl.



**Figura 7-6.** Ejemplo de un resovedor que busca un nombre remoto en 10 pasos.



**Figura 7-5.** Parte del espacio de nombres DNS dividido en zonas (la cuales están circuladas).

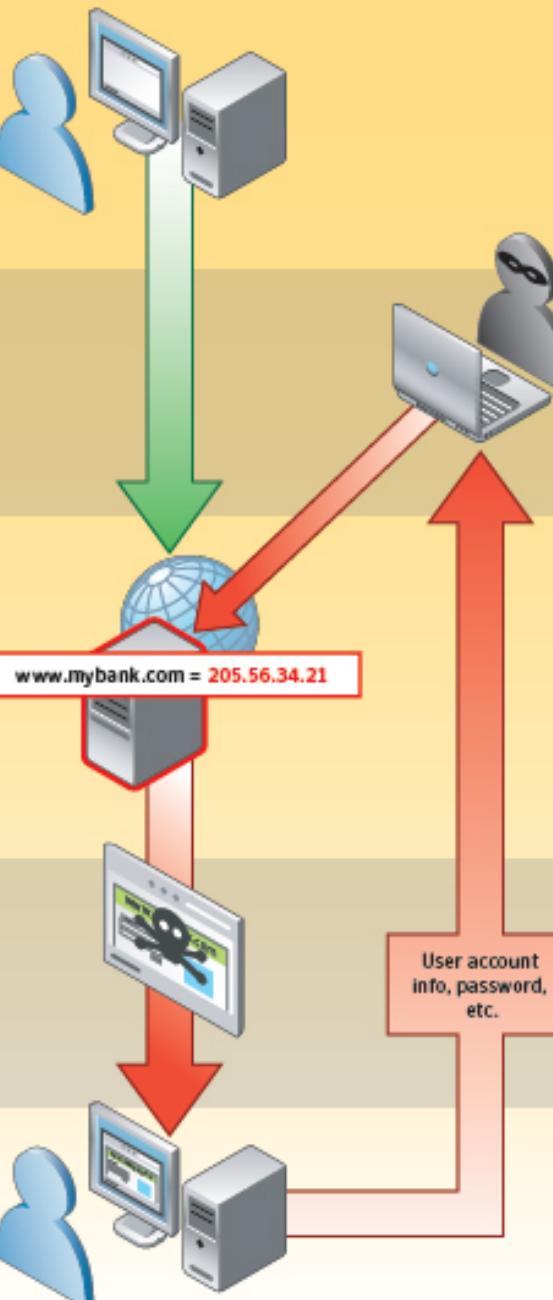
“DNS es un sistema distribuido grande y complejo, compuesto por millones de servidores de nombres que trabajan en conjunto. Forma un vínculo clave entre los nombres de dominios legibles por humanos y las direcciones IP de las máquinas. Incluye la replicación y el uso de caché para fines de desempeño y confiabilidad; además está diseñado para ser muy poderoso.”

## How Pharming Works

- 1 A person types in URL of web site they want to visit, such as [www.mybank.com](http://www.mybank.com).

The computer sends the URL request into a Domain Server.

Domain Servers are large computers that translate domain names to IP addresses.



- 2 Criminal programmers hack into the Domain Server and change the IP address for [www.mybank.com](http://www.mybank.com).

- 3 The Domain Server looks up the computer user's request for [www.mybank.com](http://www.mybank.com) and sees that the IP address is now 205.56.34.21.

This IP address is not the real IP address. It is the address that the criminals programmed.

- 4 The Domain Server directs the user's browser to a fraudulent web site. The criminals make the fraudulent web site look just like the real site.

The user is unaware they are on a fraudulent web site and types in confidential information such as their user name and password – all of which is sent directly to the criminals.

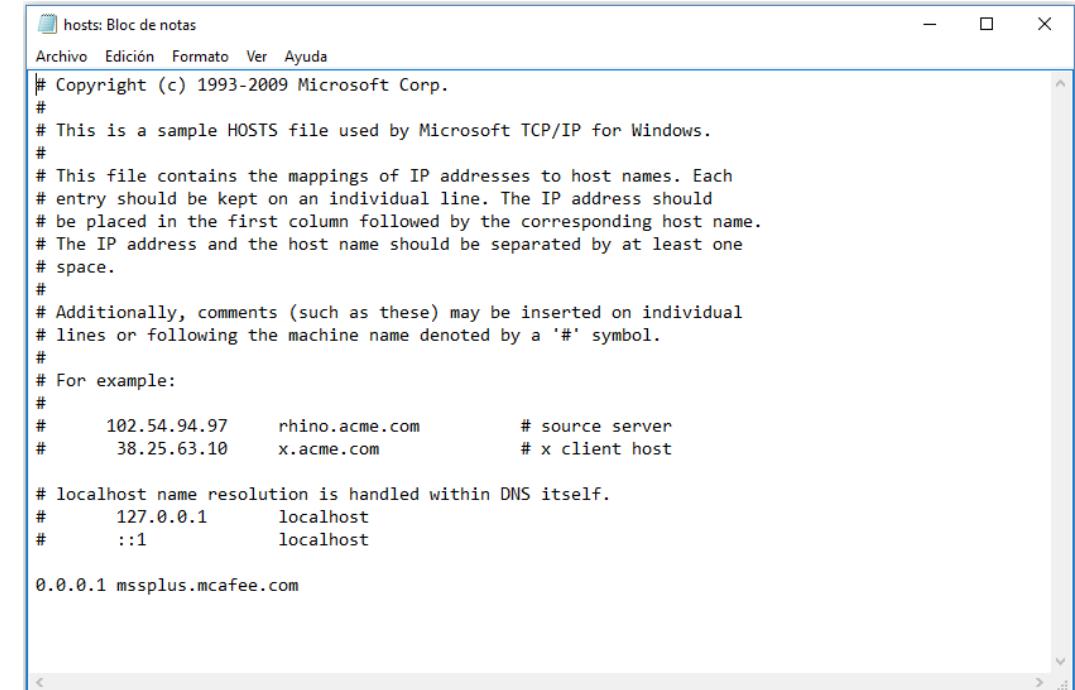
## Pharming local

*Windows 10*

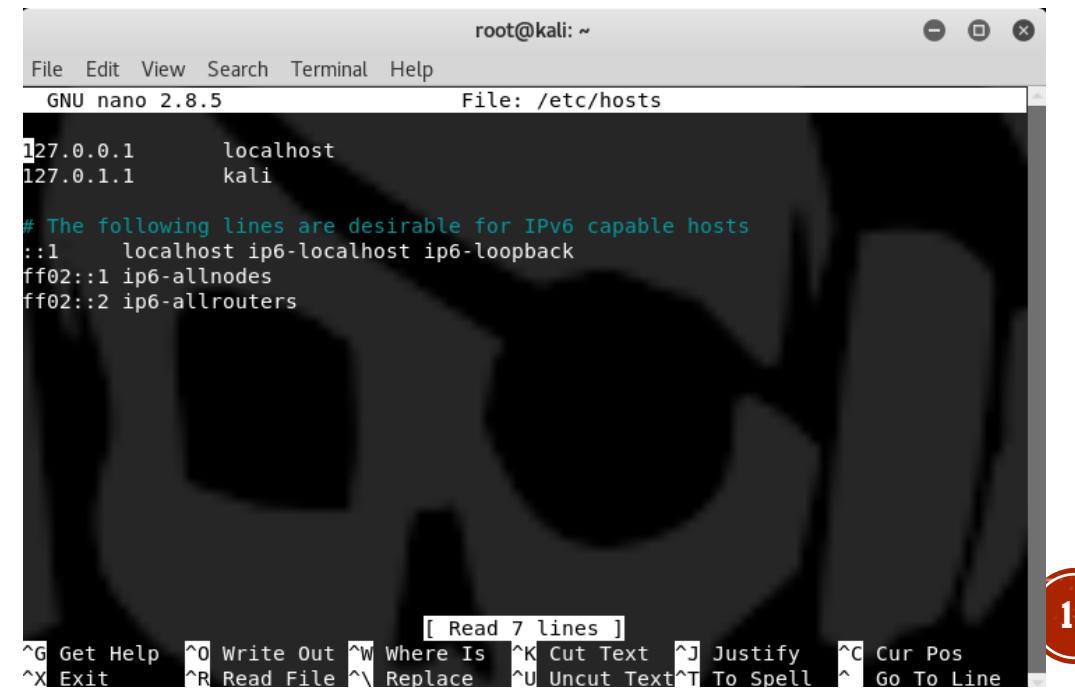
C:\Windows\System32\drivers\etc\hosts

*Linux*

/etc/hosts



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10    x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1          localhost
#      ::1                localhost
#
# 0.0.0.1 mssplus.mcafee.com
```



```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.8.5           File: /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

[ Read 7 lines ]  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ Go To Line

# CORREO ELECTRÓNICO

- Debido a que es económico y más rápido que el correo convencional, esta aplicación fue muy popular desde los primeros días de Internet.
- Antes 1990 se utilizaba en ambientes académicos, luego se dio a conocer y tuvo un impacto masivo.
- De la misma forma que el correo particular existen correos basura o **spam**.
- El correo electrónico está lleno de abreviaturas:
  - SYL (See You Later)
  - FYI (For Your Information)
- Símbolos en ASCII, conocidos como caritas (**emoticones**):
  - :-)

# CORREO ELECTRÓNICO

- Los protocolos de correo electrónico también han evolucionado, de solo realizar transferencia de archivos se han agregado características que permiten enviar correos a una lista de contactos y elementos multimedia.

## Arquitectura y servicios

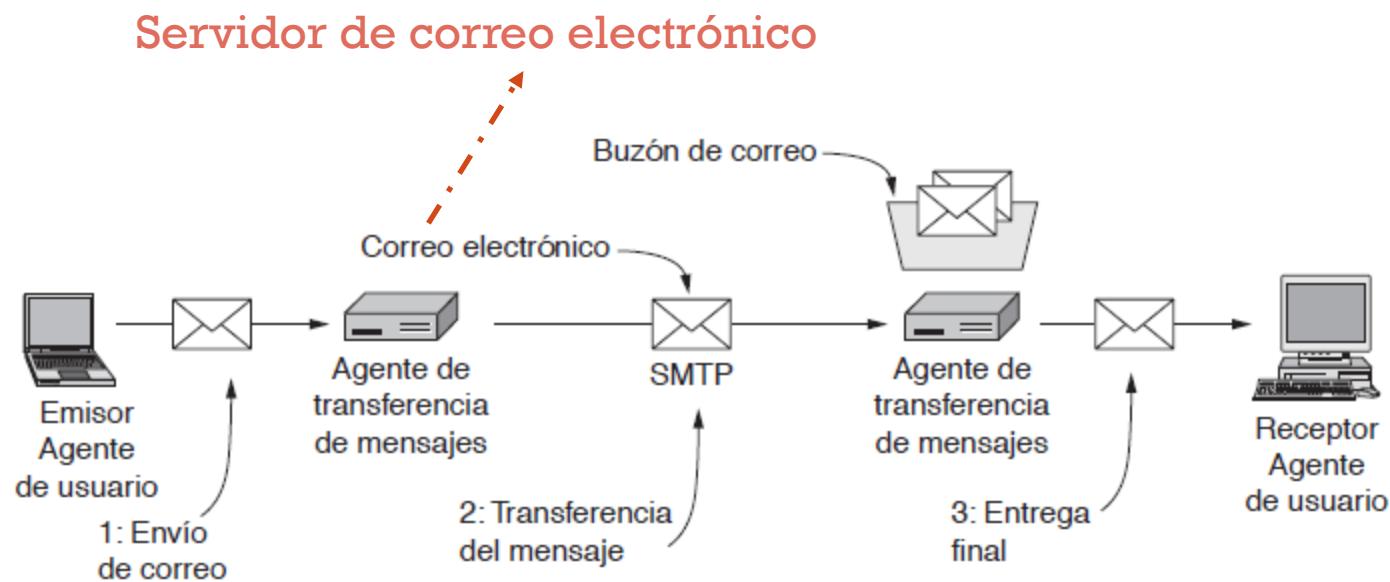
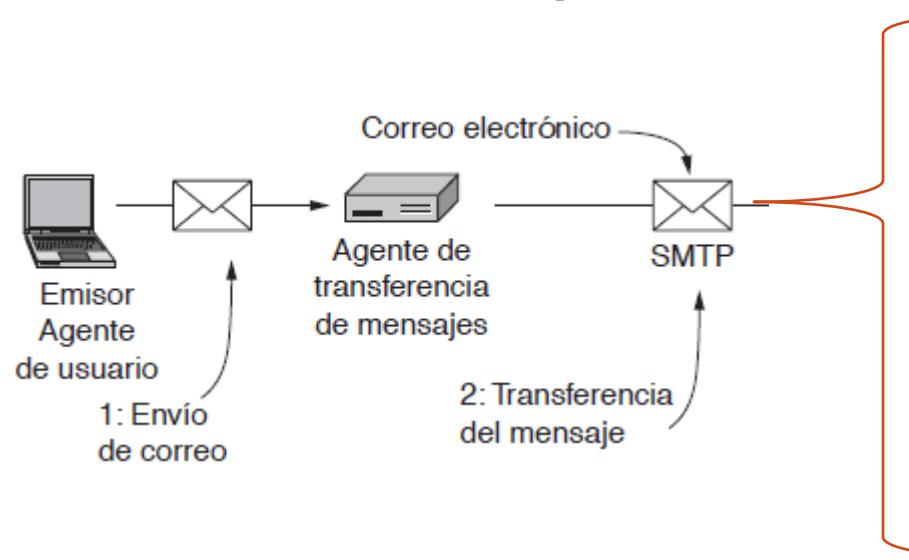


Figura 7-7. Arquitectura del sistema de correo electrónico.

# CORREO ELECTRÓNICO

- **SMTP (Simple Mail Transfer Protocol).** [RFC 5321](#)
- Vincular los agentes de usuario y de transferencia de mensajes son conceptos de los **buzones de correo** y un formato estándar de mensajes de correo electrónico.



## Envoltura

- *El encabezado – información de control para los agentes de usuario*
  - Enrutamiento
    - Dirección destino
    - Prioridad
    - Nivel de seguridad
- *Contenido – exclusivo para el destinatario humano*
  - *El cuerpo*

# CORREO ELECTRÓNICO

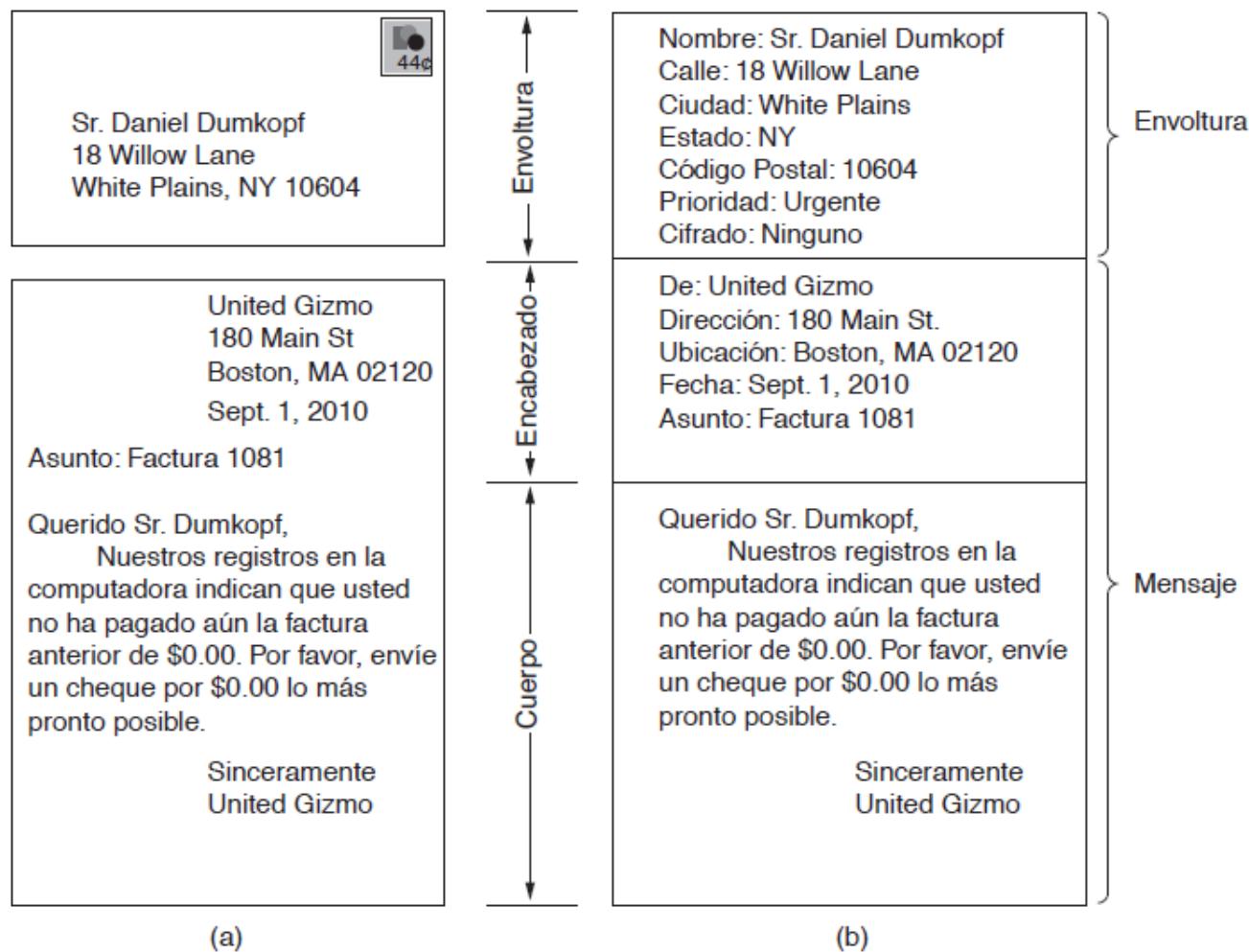


Figura 7-8. Envolturas y mensajes. (a) Correo convencional. (b) Correo electrónico.

# EL AGENTE USUARIO

- Google Gmail
- Microsoft Outlook
- Mozilla Thunderbird
- Apple Mail

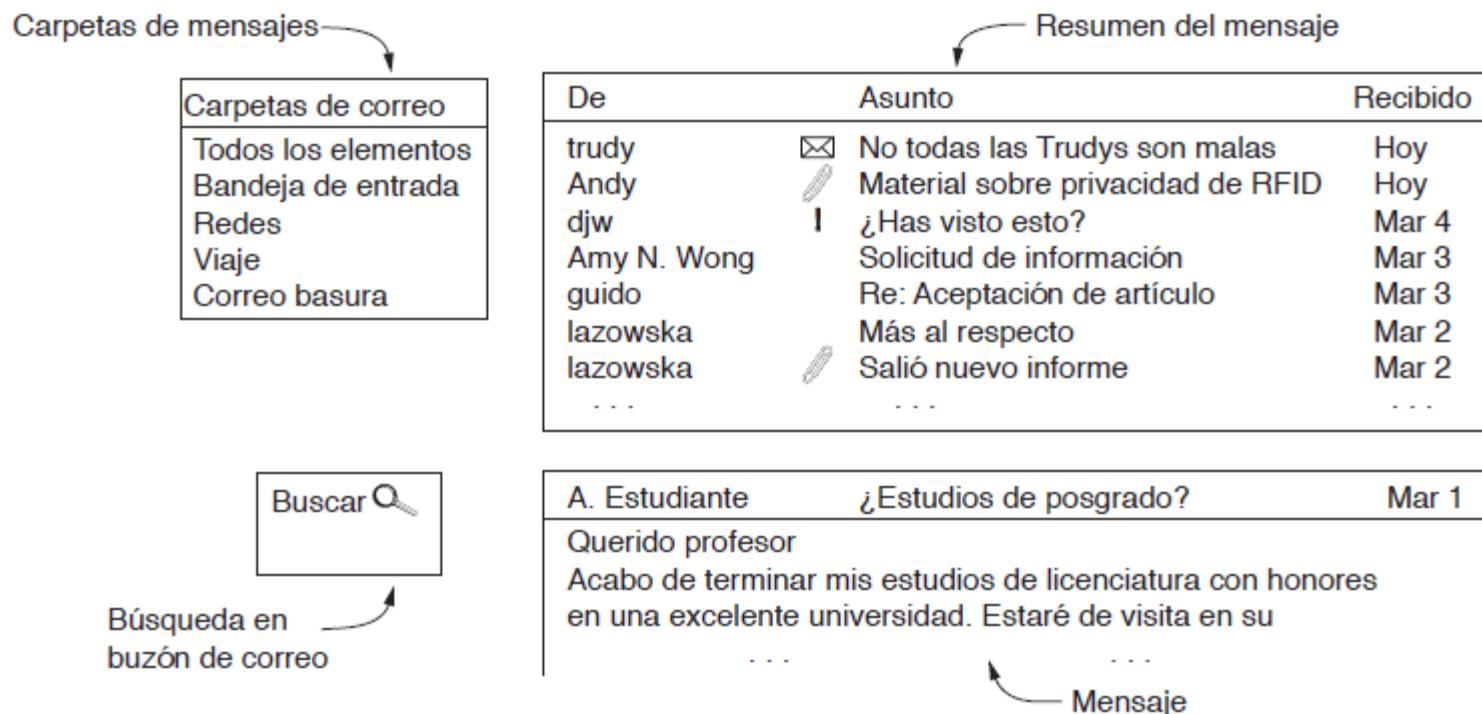


Figura 7-9. Elementos comunes de la interfaz de agente de usuario.

# FORMATOS DE MENSAJE

## RFC 5322: el formato de mensaje de Internet

- Los mensajes consisten en una envoltura primitiva (descrita como parte del SMTP en el RFC 5321), cierto número de **campos de encabezado**, una línea en blanco y después el cuerpo del mensaje. Cada campo de encabezado consiste (lógicamente) en una sola **línea de texto ASCII que contiene el nombre del campo, un signo de dos puntos y para la mayoría de los campos un valor.**

| Encabezado   | Significado  |
|--------------|--|
| To:          | Dirección(es) de correo electrónico del (los) recipiente(s) primario(s).   |
| Cc:          | Dirección(es) de correo electrónico del (los) recipiente(s) secundario(s). |
| Bcc:         | Dirección(es) de correo electrónico para las copias al carbón ocultas.     |
| From:        | Persona o personas que crearon el mensaje.                                 |
| Sender:      | Dirección de correo electrónico del emisor actual.                         |
| Received:    | Línea que agrega cada agente de transferencia a lo largo de la ruta.       |
| Return-path: | Se puede usar para identificar una ruta de vuelta al emisor.               |

Figura 7-10. Campos de encabezado del RFC 5322 relacionados con el transporte de mensajes.

| Encabezado   | Significado  |
|--------------|--|
| Date:        | Fecha y hora de envío del mensaje.                                       |
| Reply-To:    | Dirección de correo electrónico a la que se deben enviar las respuestas. |
| Message-Id:  | Número único para hacer referencia a este mensaje después.               |
| In-Reply-To: | Identificador del mensaje al que éste responde.                          |
| References:  | Otros identificadores de mensaje relevantes.                             |
| Keywords:    | Palabras clave seleccionadas por el usuario.                             |
| Subject:     | Resumen corto del mensaje para desplegar en una línea.                   |

Figura 7-11. Algunos campos utilizados en el encabezado de mensaje del RFC 5322.

# MIME: EXTENSIONES MULTIPROPÓSITO DE CORREO INTERNET

- Debido a la demanda de enviar contenido más completo a través del sistema de correo, surgieron problemas que incluían el envío y recepción de mensajes con acento, mensajes en idiomas sin alfabetos y mensajes que no contienen texto.
- **MIME (*Multipurpose Internet Mail Extensions*)** agrega una estructura al cuerpo del mensaje y definir reglas de codificación para los mensajes que no son ASCII.

| Encabezado                 | Significado   |
|----------------------------|---|
| MIME-Version:              | Identifica la versión MIME.                                       |
| Content-Description:       | Cadena legible por humanos que indica lo que contiene el mensaje. |
| Content-Id:                | Identificador único.  |
| Content-Transfer-Encoding: | Cómo se envuelve el mensaje para su transmisión.                  |
| Content-Type:              | Tipo y formato del contenido.                                     |

[https://www.w3.org/Protocols/rfc1341/5\\_Content-Transfer-Encoding.html](https://www.w3.org/Protocols/rfc1341/5_Content-Transfer-Encoding.html)

Figura 7-12. Encabezados de mensaje agregados por MIME.

| Tipo        | Subtipos de ejemplo                  | Descripción                        |
|-------------|--------------------------------------|------------------------------------|
| text        | plain, html, xml, css                | Texto en diversos formatos.        |
| image       | gif, jpeg, tiff                      | Imágenes.                          |
| audio       | basic, mpeg, mp4                     | Sonidos.                           |
| video       | mpeg, mp4, quicktime                 | Películas.                         |
| model       | vrrml                                | Modelo 3D.                         |
| application | octet-stream, pdf, javascript, zip   | Datos producidos por aplicaciones. |
| message     | http, rfc822                         | Mensaje encapsulado.               |
| multipart   | mixed, alternative, parallel, digest | Combinación de múltiples tipos.    |

Figura 7-13. Tipos de contenido MIME y subtipos de ejemplo.

<https://www.iana.org/assignments/media-types/media-types.xhtml>

# TRANSFERENCIA DE MENSAJES

From: alice@cs.washington.edu  
To: bob@ee.uwa.edu.au  
MIME-Version: 1.0  
Message-Id: <0704760941.AA00747@cs.washington.edu>  
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm  
Subject: La Tierra da vuelta al Sol un número entero de veces

Éste es el preámbulo. El agente de usuario lo ignora. Tenga un bonito día.

--qwertyuiopasdfghjklzxcvbnm  
Content-Type: text/html  
  
<p>Feliz cumpleaños a ti<br>  
Feliz cumpleaños a ti<br>  
Feliz cumpleaños, querido<b> Bob </b><br>  
Feliz cumpleaños a ti</p>

--qwertyuiopasdfghjklzxcvbnm  
Content-Type: message/external-body;  
access-type="anon-ftp";  
site="bicycle.cs.washington.edu";  
directory="pub";  
name="cumple.snd"

content-type: audio/basic  
content-transfer-encoding: base64  
--qwertyuiopasdfghjklzxcvbnm—

Figura 7-14. Un mensaje multipartita que contiene alternativas de HTML y audio.



Colombia.AI (Meetup) <colombia-ai-announce@meetup.com>  
para colombia-ai-announce ▾

5 abr. 2019 13:46



**Meetup**

 Colombia.AI (Organizador) ha enviado un mensaje  
**& Data Science | Bogotá**

Call for Speakers / Convocatoria para charlas y talleres 2019

¡Hola comunidad!

Abrimos de nuevo la convocatoria para que ustedes postulen este año. El tema deberá estar por supuesto relacionado con las charlas deben ser preferiblemente sobre **temas técnicos** y destinados a principiantes hasta avanzados. En cuanto a los talleres, se pide que sean de nivel intermedio, con **tecnologías open source**.

No tienen que ser expertos para proponer una charla, lo más importante es tener conocimientos y experiencias con la comunidad. Tampoco tienen que tener el contenido preparado para postular. De ser elegidos, les confirmaremos y los avisaremos con tiempo. Cada uno

- ← Responder
- ← Responder a todos
- Reenviar
- Filtrar mensajes como este
- Imprimir
- Añadir Colombia.AI (Meetup) a la lista de contactos
- Eliminar este mensaje
- Bloquear a Colombia.AI (Meetup)
- Marcar como spam
- Denunciar suplantación de identidad
- Mostrar original
- Traducir mensaje
- Descargar mensaje
- Marcar como no leído



## Ejemplo de Gmail

# **EXPOSICIÓN VOLUNTARIA: POP VS IMAP**

- Explicar que son IMAP Y POP:
- ¿Como se usan para la transferencia de correo?
- Ventajas y desventajas de cada uno



IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!

When you override a computer's IP configuration to point at a rogue DNS server under your control to block access to domains of your choice





<https://youtu.be/y1S5PU5LdC0>

# REFLEXIONEMOS:

- ¿Por que creen que es tan importante el sistema DNS?
- Consideran que el correo esta muerto? Si? No?  
Argumente
- ¿Saben como obtener información confiable de algún dominio?
- ¿En mi casa/trabajo quien provee el servicio de DNS? Argumente
- Comandos aprendidos y su utilidad
- Componentes del sistema DNS



<https://www.sonicwall.com/en-us/phishing-iq-test-landing>

# PLANEACIÓN

|                           |   |
|---------------------------|---|
| Material utilizado        | <ol style="list-style-type: none"><li>1. Arboleda, L. (2012). Programación en Red con Java.</li><li>2. Harold, E. (2004). Java network programming. " O'Reilly Media, Inc. ".</li><li>3. Tanenbaum, A. S. (2003). Redes de computadoras. Pearson educación.</li><li>4. Reese, R. M. (2015). Learning Network Programming with Java. Packt Publishing Ltd.</li></ol> |
| Actividades DESPUÉS clase |   |