

REDES DE COMPUTADORES Y LABORATORIO

Christian Camilo Urcuqui López, MSc



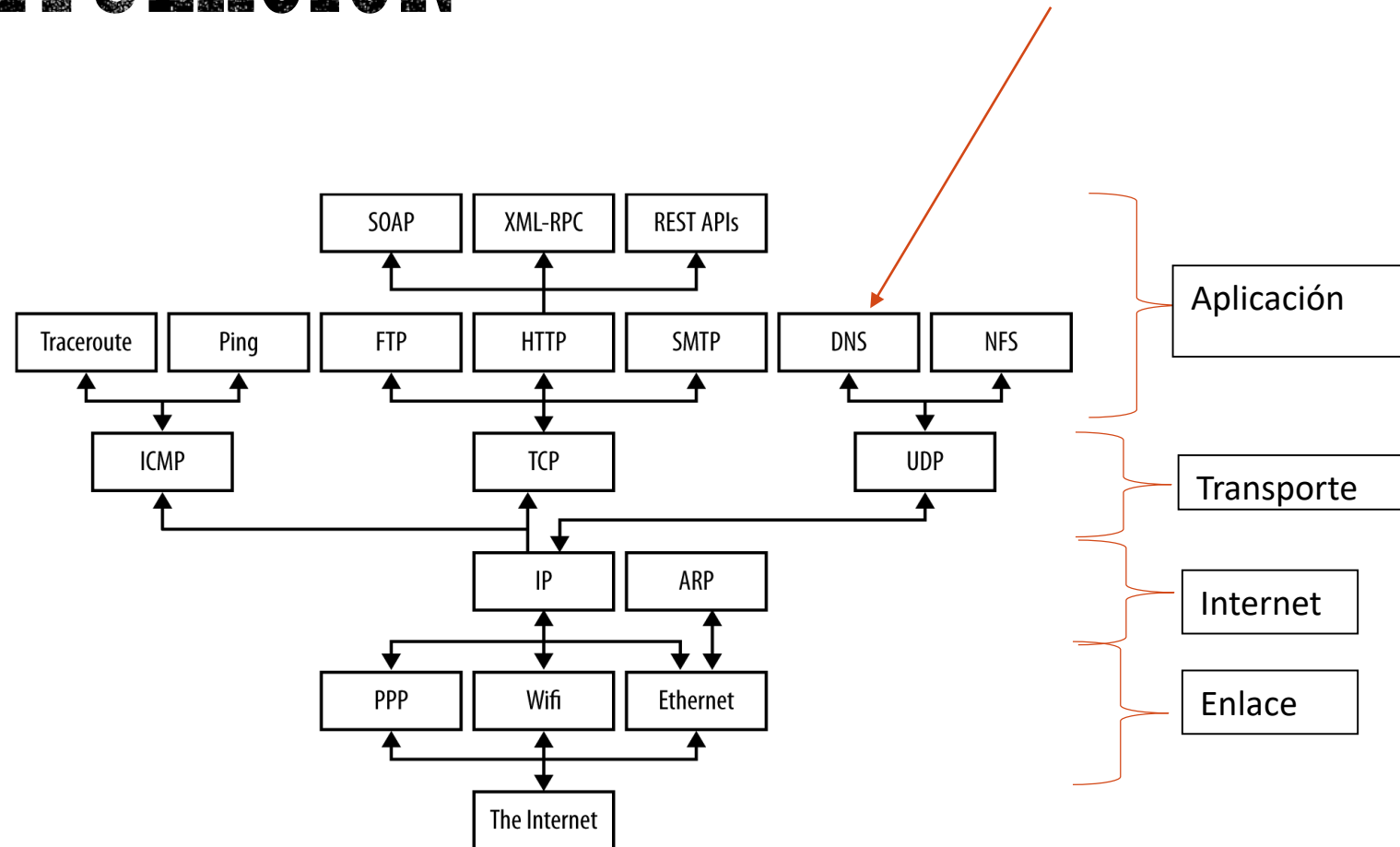
BIBLIOGRAFÍA



COMPETENCIAS

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

RECAPITULACIÓN



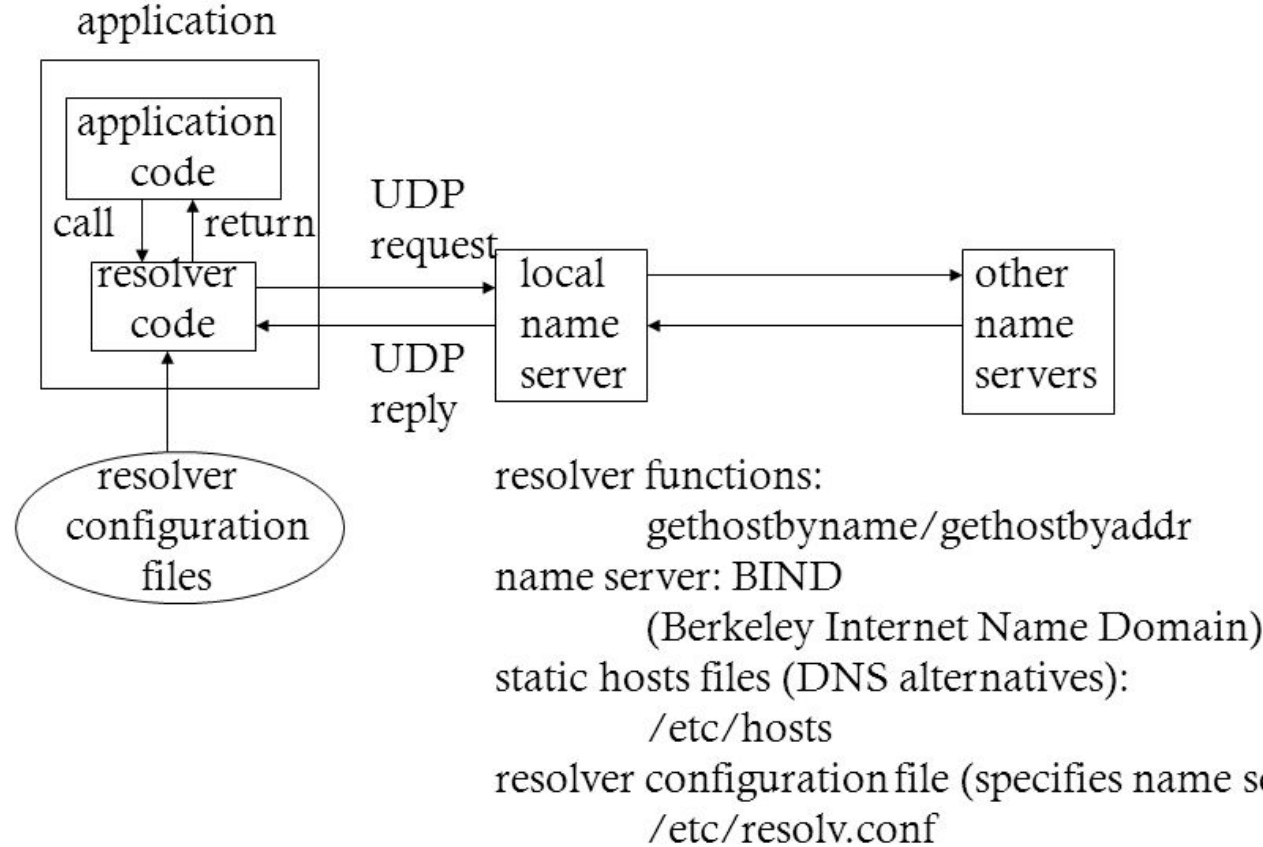
LA CAPA DE APLICACIÓN

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.
- Como hemos mencionado, 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.
- Recordemos que DNS es un esquema jerárquico de nombres basado en dominios y un sistema de base de datos destruido. ([RFC 1034](#), [1035](#), [2181](#))

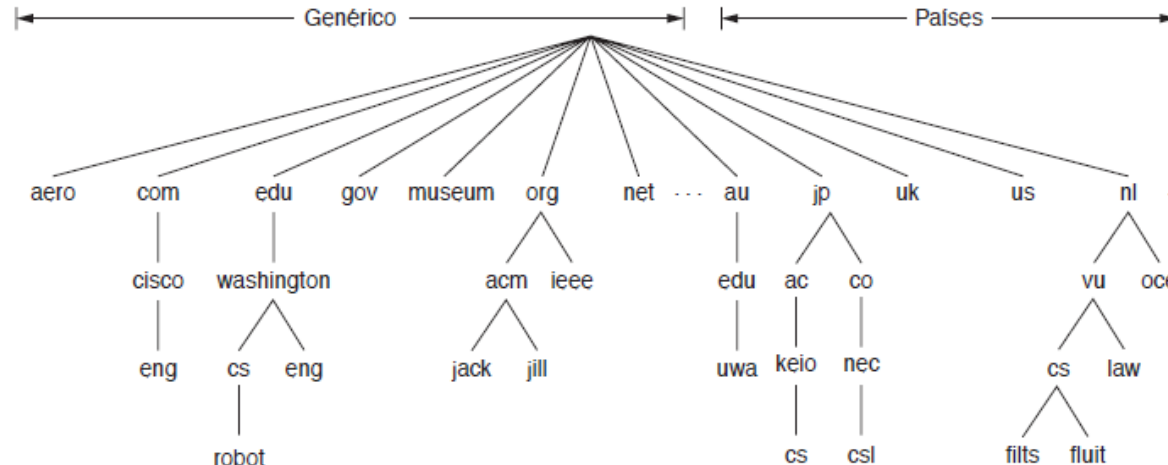
DNS: Application, Resolver, Name Servers

Resolución de nombres



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*).



icesi.edu.co

i2t.icesi.edu.co

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 **resolvedor** asigna un nombre de dominio al DNS, lo que recibe son los registros de recursos asociados a ese nombre.

<i>Nombre_dominio</i>	<i>Tiempo_de_vida</i>	<i>Clase</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.

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

<i>Tipo</i>	<i>Valor</i>
; 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 7-4. Parte de una posible base de datos DNS para cs.vu.nl.

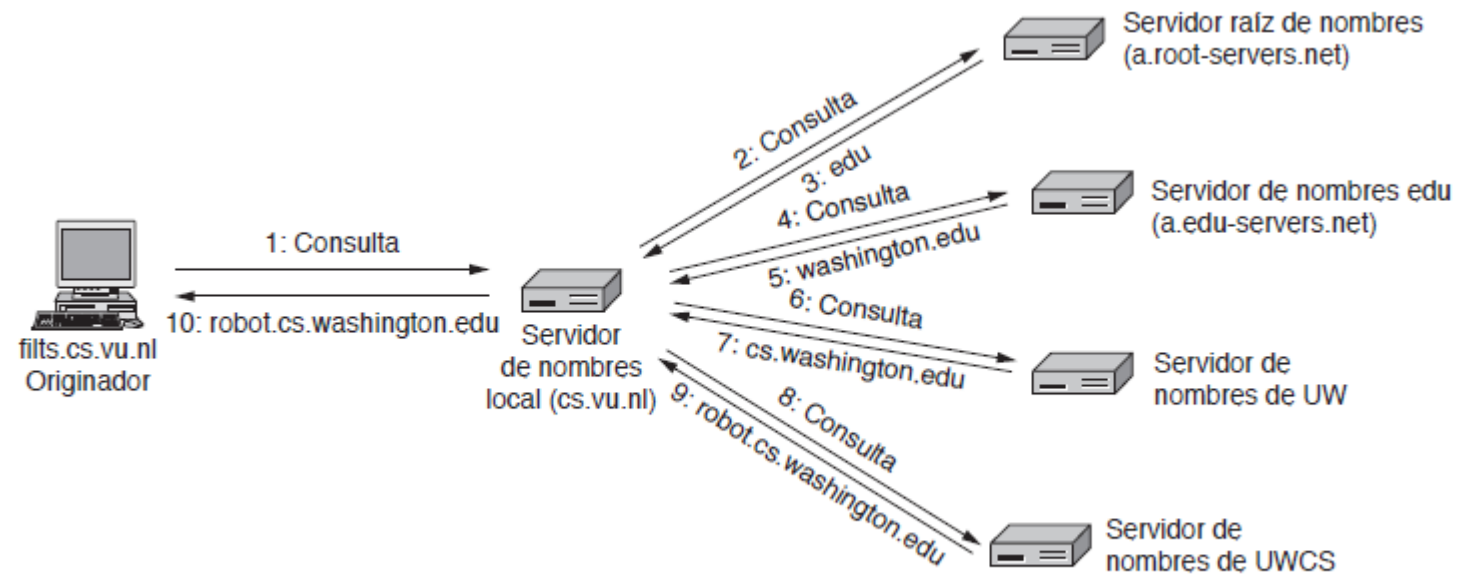


Figura 7-6. Ejemplo de un resolvidor que busca un nombre remoto en 10 pasos.

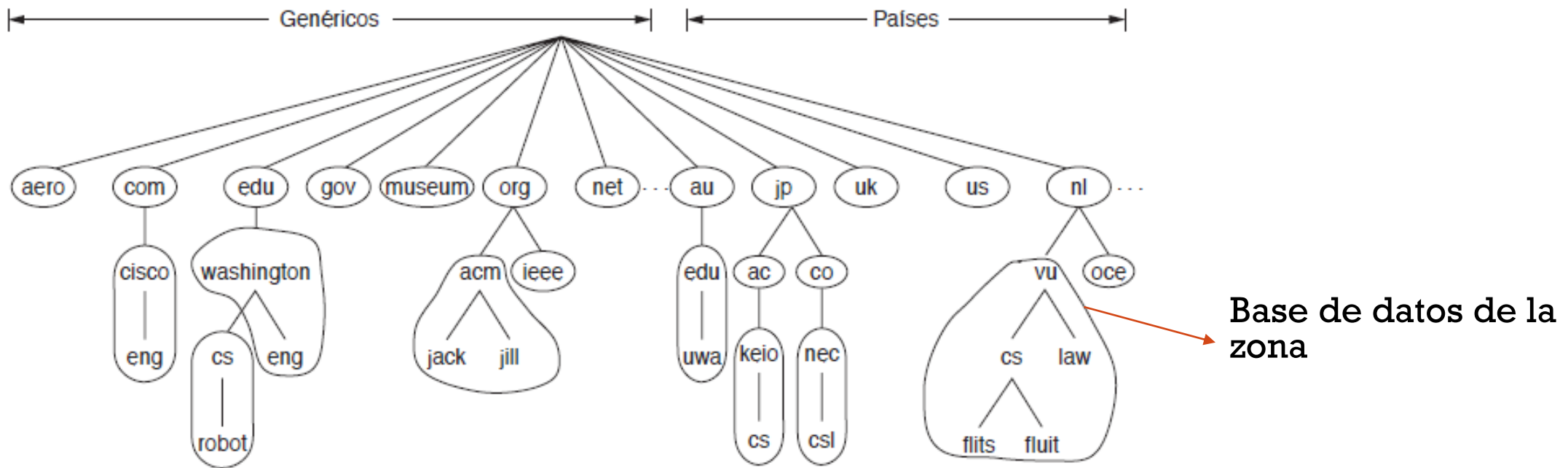


Figura 7-5. Parte del espacio de nombres DNS dividido en zonas (la cuales están circuladas).

“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.

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.



- 3 The Domain Server looks up the computer user's request for 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.



User account info, password, etc.

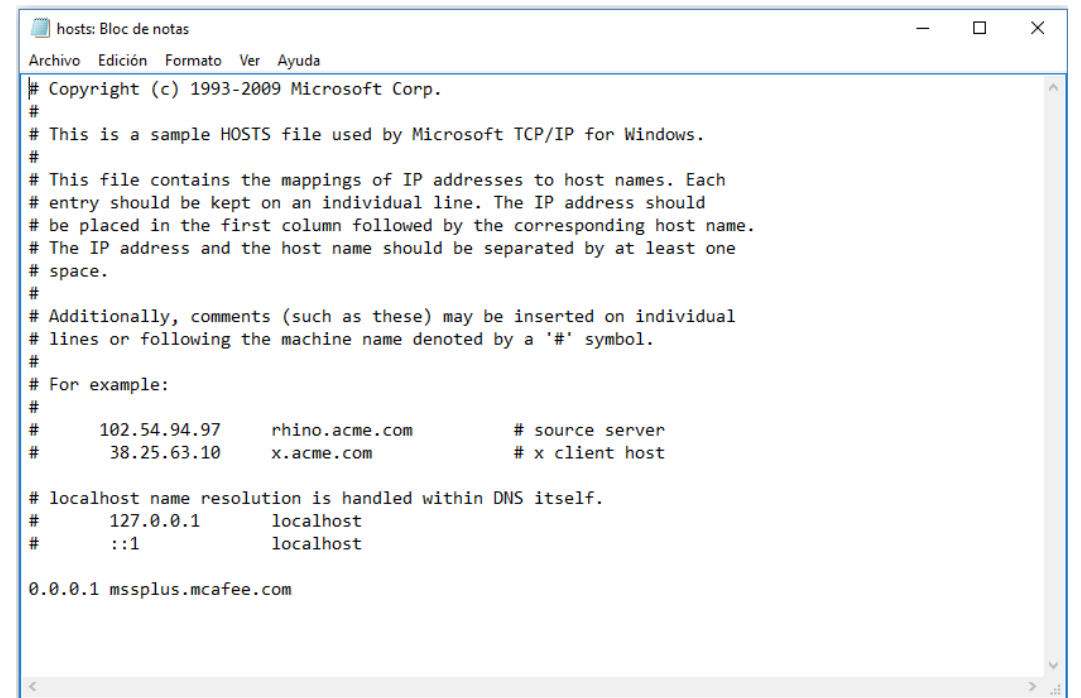
Pharming local

Windows 10

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

Linux

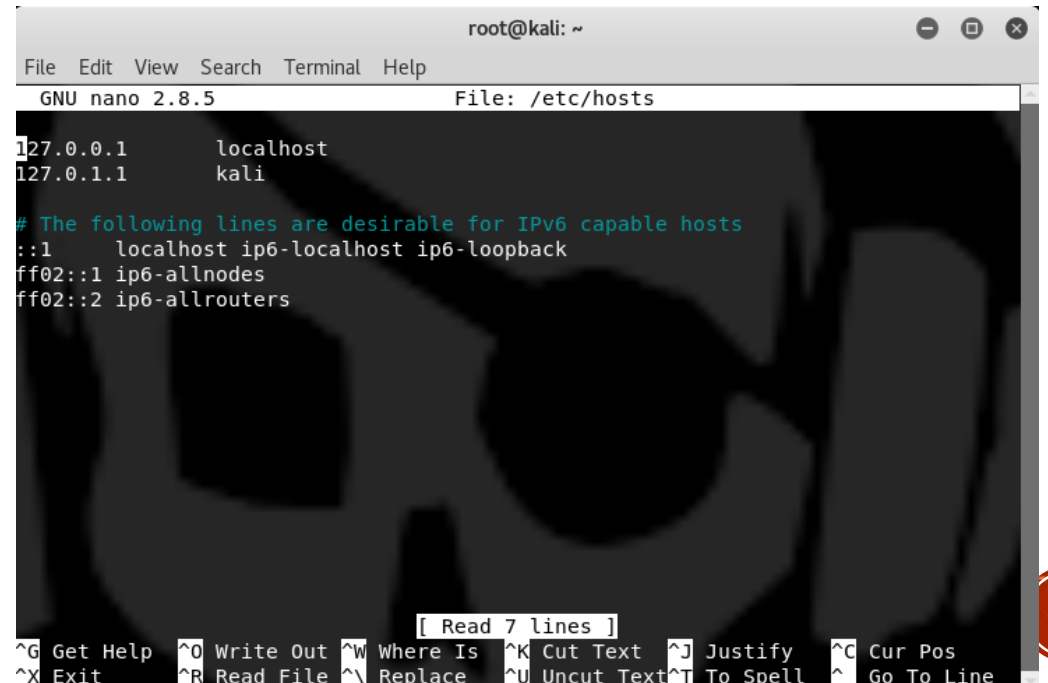
/etc/hosts



```
hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# 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
```

CORRE 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**):
 - :-)

CORRE 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

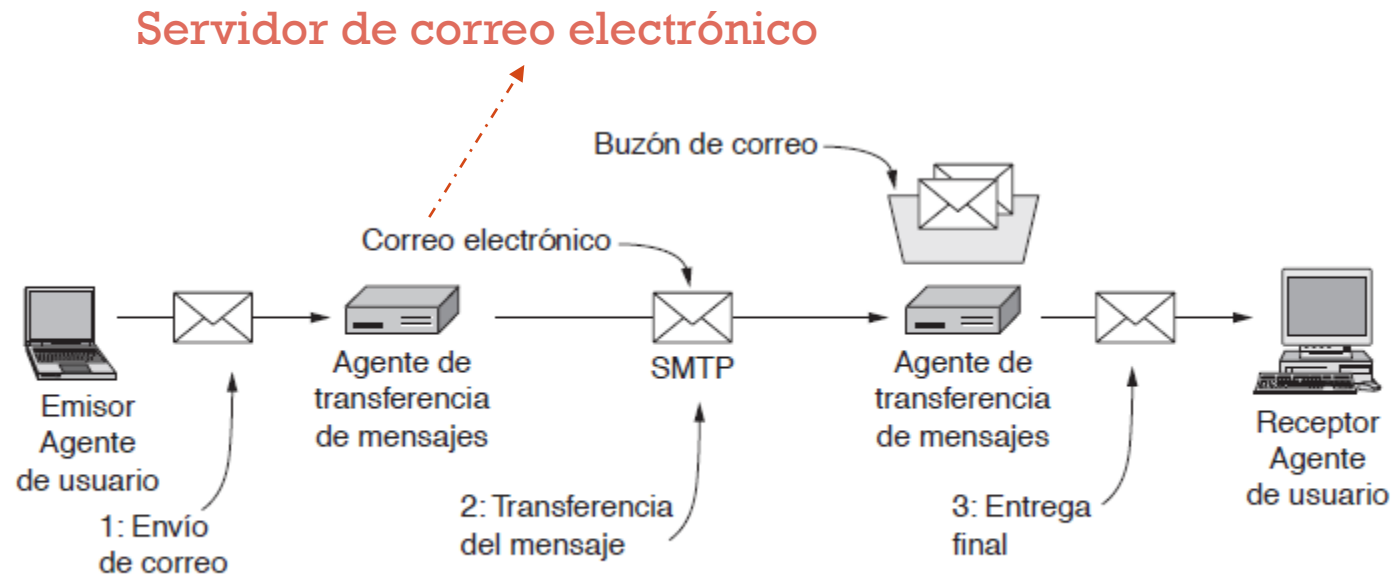
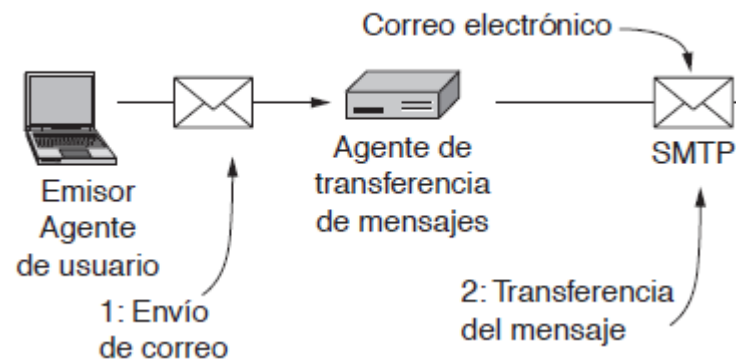


Figura 7-7. Arquitectura del sistema de correo electrónico.

CORRE 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

CORRE ELECTRÓNICO

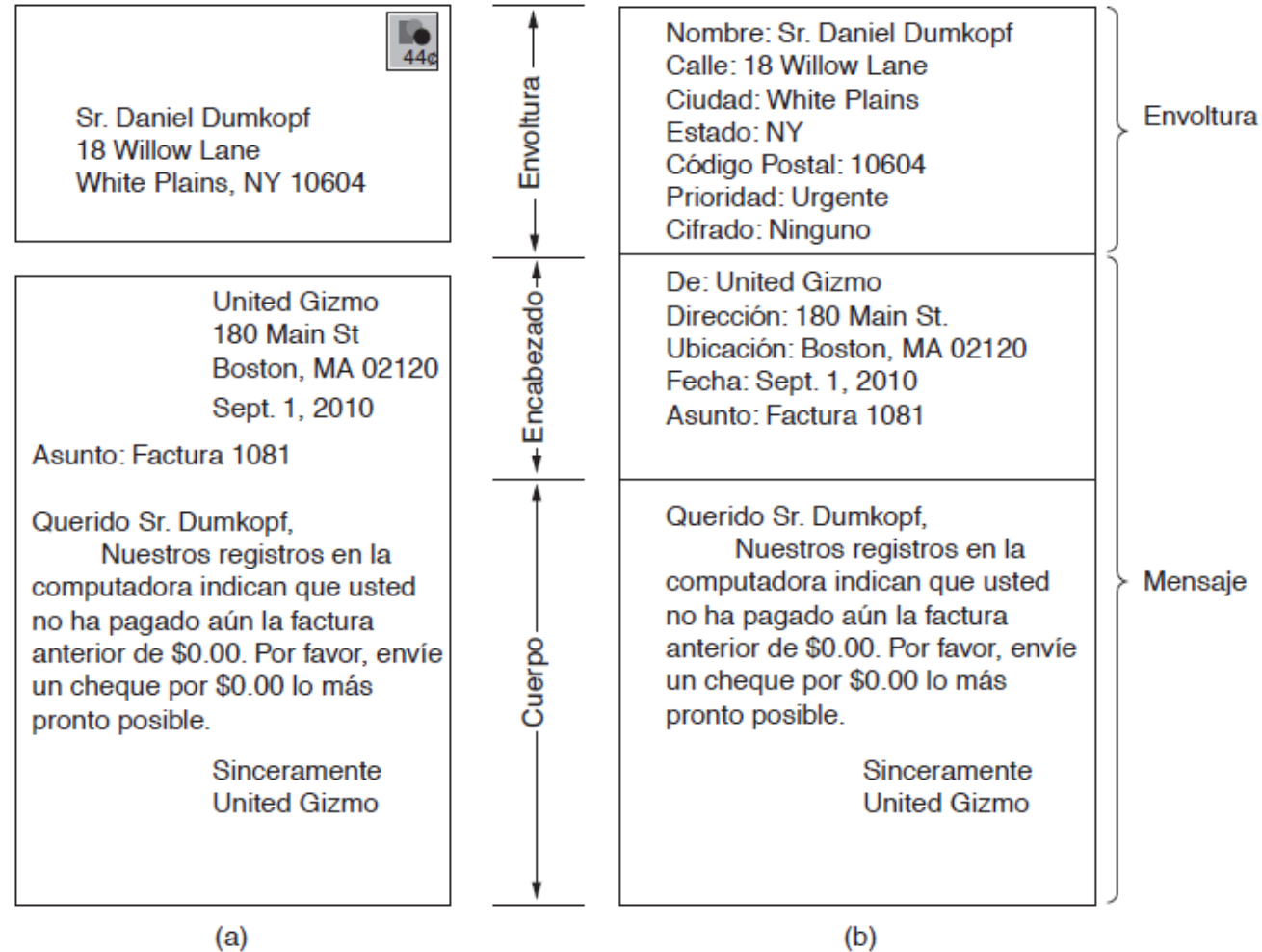


Figura 7-8. Envolturas y mensajes. (a) Correo convencional. (b) Correo electrónico.

EL AGENTE USUARIO

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

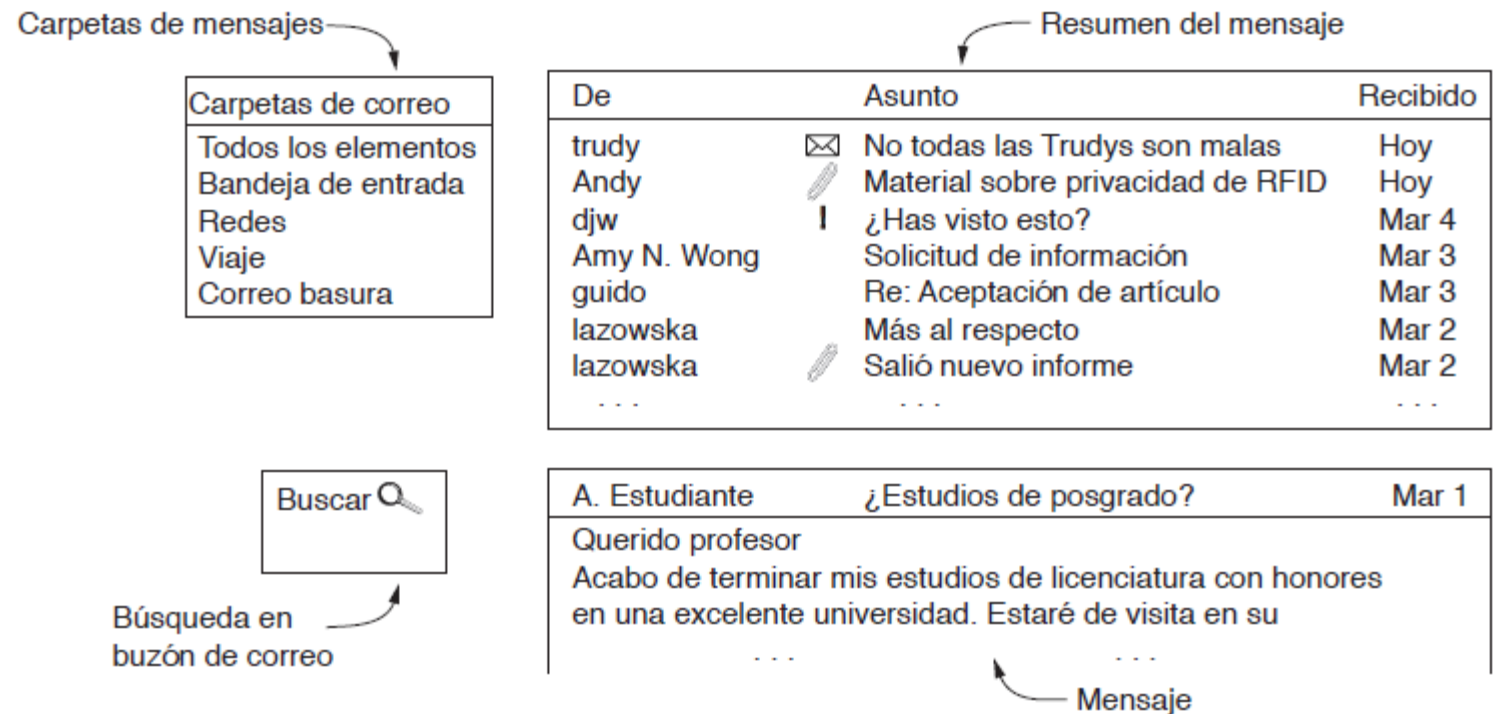


Figura 7-9. Elementos comunes de la interfaz de agente de usuario.

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

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	vrml	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

Feliz cumpleaños a ti

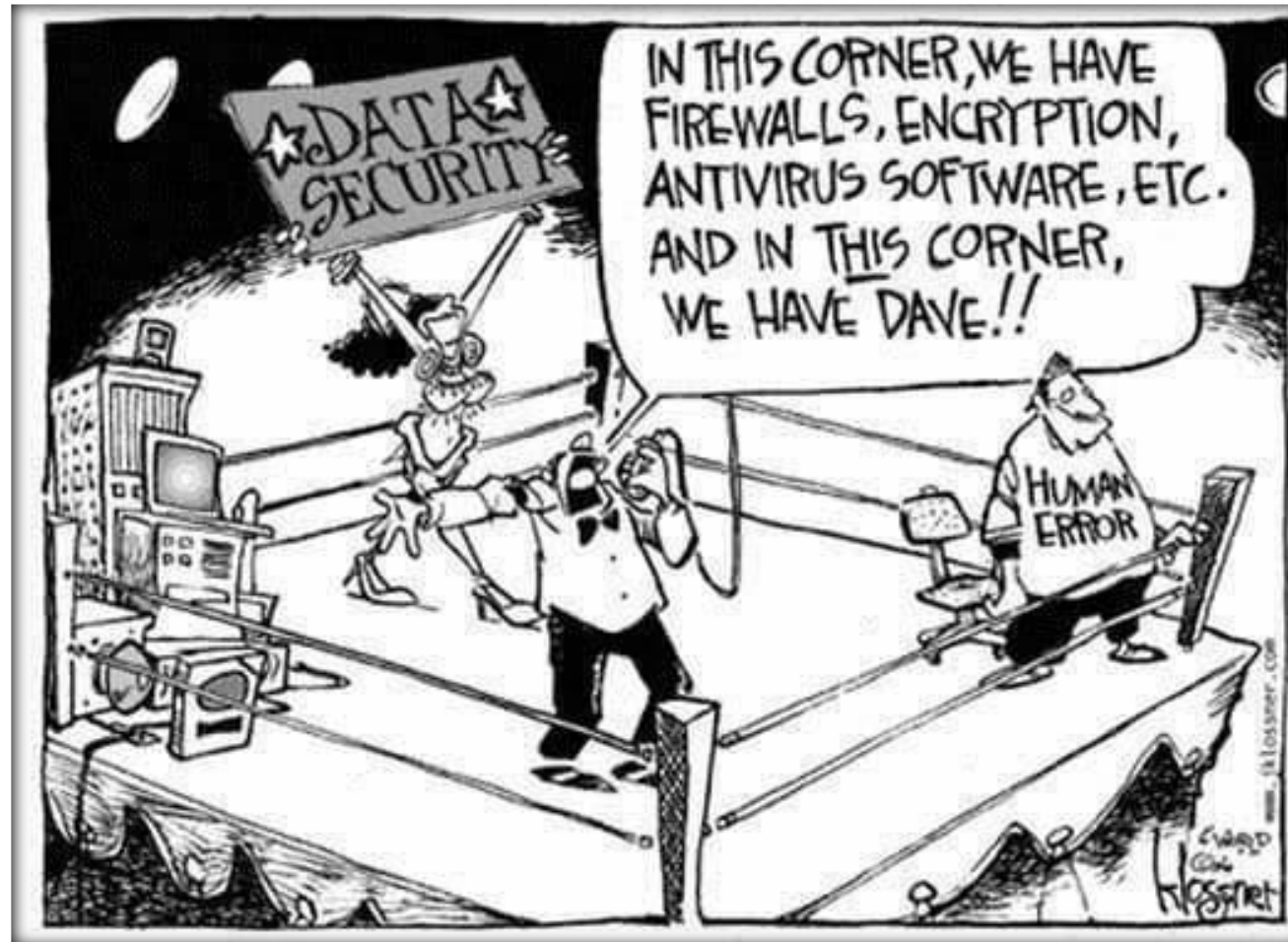
Feliz cumpleaños, querido Bob

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.





<https://youtu.be/y1S5PU5LdC0>



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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Micro-St_14:84:e4	LLDP_Multicast	LLDP	58	TTL = 3601
2	0.007629	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xb40a60f7
3	0.008105	Micro-St_14:84:e4	Broadcast	ARP	42	Who has 172.16.32.1? Tell 172.16.32.152
4	0.168291	Micro-St_14:84:e4	Broadcast	ARP	42	Who has 172.16.32.152? Tell 0.0.0.0
5	0.168466	172.16.32.152	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
6	0.356980	::	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
7	0.587340	::	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
8	0.667245	::	ff02::1:ffa6:d70b	ICMPv6	78	Neighbor Solicitation for fe80::213:37ff:fea6:d70b
9	0.668238	Micro-St_14:84:e4	Broadcast	ARP	42	Who has 172.16.32.1? Tell 172.16.32.152
10	0.668300	172.16.32.152	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
11	0.668497	OrientPo_a6:d7:0b	Micro-St_14:84:e4	ARP	60	172.16.32.1 is at 00:13:37:a6:d7:0b
• 12	0.763507	172.16.32.152	172.16.32.1	DNS	77	Standard query 0x8aba A wpad.icesi.edu.co

▼ Domain Name System (response)	
Transaction ID: 0xd294	
> Flags: 0x8580 Standard query response, No error	
Questions: 1	
Answer RRs: 1	
Authority RRs: 0	
Additional RRs: 0	
▼ Queries	
▼ wpad.icesi.edu.co: type A, class IN	
Name: wpad.icesi.edu.co	
[Name Length: 17]	
[Label Count: 4]	
Type: A (Host Address) (1)	
Class: IN (0x0001)	
▼ Answers	
> wpad.icesi.edu.co: type A, class IN, addr 127.0.0.1	
[Request In: 41]	
[Time: 2.001381000 seconds]	
0000	30 9c 23 14 84 e4 00 13 37 a6 d7 0b 08 00 45 00 0·#····· 7·····E·
0010	00 4f 6c 6c 40 00 40 11 35 78 ac 10 20 01 ac 10 ·0ll@·@· 5x·· ···
0020	20 98 00 35 eb fd 00 3b bd a6 d2 94 85 80 00 01 ··5····; ······
0030	00 01 00 00 00 00 04 77 70 61 64 05 69 63 65 73 ······w pad·ices
0040	69 03 65 64 75 02 63 6f 00 00 01 00 01 c0 0c 00 i·edu·co ······
0050	01 00 01 00 00 00 00 00 04 7f 00 00 01 ······ ······